AssuredSAN 3000 Series
RAIDar User Guide

P/N 83-00005970-13-01
Revision A
May 2011

Copyright © 2011 Dot Hill Systems Corp. All rights reserved. Dot Hill Systems Corp., Dot Hill, the Dot Hill logo, AssuredSAN, AssuredSnap, AssuredCopy, AssuredRemote, EcoStor, SimulCache, R/Evolution, and the R/Evolution logo are trademarks of Dot Hill Systems Corp. All other trademarks and registered trademarks are proprietary to their respective owners.

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, changes in the product design can be made without reservation and without notification to its users.

Contents

About this guide . . . 13
Intended audience . . . 13
Prerequisites . . . 13
Related documentation . . . 13
Related documentation . . . 13
Document conventions and symbols . . . 14

1 Getting started . . . 15
Configuring and provisioning a new storage system . . . 15
Browser setup . . . 15
Signing in . . . 15
Tips for signing in and signing out . . . 16
Tips for using the main window . . . 16
Tips for using the help window . . . 17
System concepts . . . 17
About user accounts . . . 17
Related topics . . . 18
About vdisks . . . 18
Related topics . . . 19
About spares . . . 19
Related topics . . . 19
About volumes . . . 20
Related topics . . . 20
About hosts . . . 20
Related topics . . . 21
About volume mapping . . . 21
Related topics . . . 22
About volume cache options . . . 22
Using write-back or write-through caching . . . 22
Optimizing read-ahead caching . . . 23
Related topics . . . 23
About managing remote systems . . . 24
Related topics . . . 24
About the Snapshot feature . . . 24
Related topics . . . 26
About the Volume Copy feature . . . 26
Related topics . . . 28
About the AssuredRemote replication feature . . . 28
About the VDS and VSS hardware providers . . . 28
About RAID levels . . . 28
About size representations . . . 30
Related topics . . . 30
About the system date and time . . . 30
Related topics . . . 31
About storage-space color codes . . . 31
About Configuration View icons . . . 31
About vdisk reconstruction . . . 31
About data protection in a single-controller storage system . . . 32

2 Configuring the system . . . 33
Using the Configuration Wizard . . . 33
Step 1: Starting the wizard . . . 33
Step 2: Changing default passwords . . . 33
Step 3: Configuring network ports . . . 33
Step 4: Enabling system-management services . . . 34
Step 5: Setting system information . . . 35
Step 6: Configuring event notification . . . 35
Step 7: Configuring host ports . . . 35
Step 8: Confirming configuration changes . . . 37
Installing a license . . . 37
Configuring system services . . . 38
Changing management interface settings . . . 38
Configuring email notification . . . 39
Configuring SNMP notification . . . 39
Configuring user accounts . . . 40
Adding users . . . 40
Modifying users . . . 41
Removing users . . . 41
Configuring system settings . . . 42
Changing the system date and time . . . 42
Changing host interface settings . . . 42
Changing network interface settings . . . 44
Setting system information . . . 45
Configuring advanced settings . . . 45
Changing disk settings . . . 45
Configuring SMART . . . 45
Configuring dynamic spares . . . 45
Configuring drive spin down for available disks and global spares . . . 45
Scheduling drive spin down for all disks . . . 46
Configuring the EMP polling rate . . . 46
Changing system cache settings . . . 47
Changing the synchronize-cache mode . . . 47
Changing the missing LUN response . . . 47
Controlling host access to the system's write-back cache setting . . . 47
Changing auto-write-through cache triggers and behaviors . . . 48
Configuring partner firmware update . . . 48
Configuring system utilities . . . 48
Configuring background scrub for vdisks . . . 48
Configuring background scrub for disks not in vdisks . . . 49
Configuring utility priority . . . 49
Configuring remote systems . . . 50
Adding a remote system . . . 50
Deleting remote systems . . . 50
Configuring a vdisk . . . 50
Managing dedicated spares . . . 50
Changing a vdisk's name . . . 51
Changing a vdisk's owner . . . 51
Configuring drive spin down for a vdisk . . . 51
Configuring a volume . . . 52
Changing a volume's name . . . 52
Changing a volume's cache settings . . . 52
Configuring a snapshot . . . 53
Changing a snapshot's name . . . 53
Configuring a snap pool . . . 53
Changing a snap pool's name . . . 53

3 Provisioning the system 55
Using the Provisioning Wizard 55
Step 1: Starting the wizard 55
Step 2: Specifying the vdisk name and RAID level 55
Step 3: Selecting disks 56
Step 4: Defining volumes 56
Step 5: Setting the default mapping 57
Step 6: Confirming vdisk settings 57
Creating a vdisk 57
Deleting vdisks 58
Managing global spares 58
Creating a volume set 59
Creating a volume 59
Deleting volumes 60
Changing default mapping for multiple volumes 60
Explicitly mapping multiple volumes 61
Changing a volume's default mapping 62
Changing a volume's explicit mappings 63
Unmapping volumes 64
Expanding a volume 64
Creating multiple snapshots 64
Creating a snapshot 65
Deleting snapshots 65
Resetting a snapshot 66
Creating a volume copy 67
Aborting a volume copy 68
Rolling back a volume 68
Creating a snap pool 69
Deleting snap pools 70
Adding a host 70
Removing hosts 70
Changing a host's name 70
Changing host mappings 71
Configuring CHAP 72
Modifying a schedule 72
Deleting schedules 73
4 Using system tools 75
Updating firmware 75
Updating controller-module firmware 75
Updating expansion-module firmware 76
Updating disk firmware 77
Saving logs 78
Resetting a host port 78
Rescanning disk channels 79
Restoring system defaults 79
Clearing disk metadata 79
Restarting or shutting down controllers 80
Restarting 80
Shutting down 81
Testing event notification 81
Expanding a vdisk 81
Verifying a vdisk 82
Scrubbing a vdisk 82
Removing a vdisk from quarantine 83
Expanding a snap pool 84
Checking links to a remote system 85
Checking links in the local system 85

5 Viewing system status . . . 87
Viewing information about the system . . . 87
System properties . . . 87
Enclosure properties . . . 87
Disk properties . . . 87
Vdisk properties . . . 87
Volume properties . . . 87
Snap-pool properties . . . 87
Snapshot properties . . . 88
Schedule properties . . . 88
Configuration limits . . . 88
Licensed features . . . 88
Version properties . . . 88
Viewing the system event log . . . 88
Viewing information about all vdisks . . . 89
Viewing information about a vdisk . . . 90
Vdisk properties . . . 90
Disk properties . . . 91
Volume properties . . . 92
Snap-pool properties . . . 92
Viewing information about a volume . . . 92
Volume properties . . . 93
Mapping properties . . . 93
Schedule properties . . . 93
Viewing information about a snapshot . . . 94
Snapshot properties . . . 94
Mapping properties . . . 95
Schedule properties . . . 95
Viewing information about a snap pool . . . 96
Snap-pool properties . . . 96
Volume properties . . . 97
Snapshot properties . . . 97
Viewing information about all hosts . . . 97
Viewing information about a host . . . 97
Host properties . . . 97
Mapping properties . . . 98
Viewing information about an enclosure . . . 98
Enclosure properties . . . 98
Disk properties . . . 99
Power supply properties . . . 100
Controller module properties . . . 100
Controller module: network port properties . . . 101
Controller module: host port properties . . . 101
Controller module: expansion port properties . . . 101
Controller module: CompactFlash properties . . . 102
Drive enclosure: I/O module properties . . . 102
I/O module: In port properties . . . 102
I/O module: Out port properties . . . 102
Viewing information about a remote system . . . 103
6 Using AssuredRemote to replicate volumes . . . 105
About the AssuredRemote replication feature . . . 105
Replication process overview . . . 105
Replication actions . . . 107
Performing initial replication locally or remotely . . . 108
Remote replication disaster recovery . . . 109
Remote replication licensing . . . 110
Related topics . . . 110

Using the Replication Setup Wizard . . . 110
Step 1: Starting the wizard . . . 111
Step 2: Selecting the primary volume . . . 111
Step 3: Selecting the replication mode . . . 111
Step 4: Selecting the secondary volume . . . 112
Step 5: Confirming replication settings . . . 112
Replicating a volume . . . 112
Replicating a snapshot . . . 114
Removing replication from a volume . . . 114
Suspending replication . . . 115
Resuming replication . . . 115
Aborting replication . . . 115
Detaching a secondary volume . . . 115
Stopping a vdisk . . . 116
Starting a vdisk . . . 117
Reattaching a secondary volume . . . 117
Exporting a replication image to a snapshot . . . 118
Changing the primary volume for a replication set . . . 118
Viewing replication properties, addresses, and images for a volume . . . 119
Replication properties . . . 120
Replication addresses . . . 120
Replication images . . . 121
Viewing information about a remote primary or secondary volume . . . 121
Replication properties . . . 121
Replication addresses . . . 121
Replication image properties . . . 121
Viewing information about a replication image . . . 121
Replication status properties . . . 122
Primary volume snapshot properties . . . 122
Secondary volume snapshot properties . . . 122

A SNMP reference . . . 123
Standard MIB-II behavior . . . 123
Enterprise traps . . . 123
FA MIB 2.2 SNMP behavior . . . 123
External details for certain FA MIB 2.2 objects . . . 129
External details for connUnitRevsTable . . . 129
External details for connUnitSensorTable . . . 130
External details for connUnitPortTable . . . 131
Configuring SNMP event notification in RAIDar . . . 131
SNMP management . . . 131
Enterprise trap MIB . . . 131

B Using FTP to download logs and update firmware . . . 135
Downloading system logs . . . 135
Updating firmware . . . 136
Updating controller-module firmware . . . 136
Updating expansion-module firmware . . . 137
Updating disk firmware . . . 139
Installing a license file . . . 140

C Using SMI-S . . . 141
SMI-S overview . . . 141
Key components . . . 141
WBEM . . . 141
CIM . . . 141
SLP . . . 141
Profiles . . . 141
SMI-S implementation . . . 142
About the 3000 Series SMI-S provider . . . 142

SMI-S profiles . . . 143
CIM Alerts . . . 144
SMI-S configuration . . . 144
Frequently asked questions . . . 145
What is an embedded SMI-S array provider? . . . 145
How do I test SMI-S? . . . 145
What storage arrays are supported? . . . 145
What's new in this release? . . . 146
What is the architecture? . . . 146
What CIM operations are supported? . . . 146
Is the product CTP-certified? . . . 147
Troubleshooting . . . 147
Definitions . . . 147
Block Server Performance subprofile . . . 147
LUN Masking and Mapping operations . . . 147
Alert Indications . . . 148
Full provisioning . . . 148
Replication support . . . 148
What is the codebase for the CIM clients? . . . 148
Glossary . . . 149
Index . . . 153

Figures

1 Relationship between a master volume and its snapshots and snap pool 24
2 Rolling back a master volume 25
3 Creating a volume copy from a master volume or a snapshot 27
4 Intersite and intrasite replication sets 106
5 Actions that occur during a series of replications 107
6 Example of primary-volume failure 109

Tables

1 Document conventions 14
2 RAIDar communication status icons 16
3 Settings for default users 18
4 Example applications and RAID levels 28
5 RAID level comparison 29
6 Vdisk expansion by RAID level 29
7 Size representations in base 2 and base 10 30
8 Decimal (radix) point character by locale 30
9 Storage-space color codes 31
10 Configuration View icons 31
11 FA MIB 2.2 objects, descriptions, and values 124
12 connUnitRevsTable index and description values 129
13 connUnitSensorTable index, name, type, and characteristic values. 130
14 connUnitPortTable index and name values 131
15 Supported SMI-S profiles. 143
16 CIM Alert indication events 144

About this guide

This guide provides information about managing an AssuredSAN™ 3000 Series storage system by using its web interface, RAIDar Storage Management Utility.

Intended audience

This guide is intended for storage system administrators.

Prerequisites

Prerequisites for using this product include knowledge of:

- Network administration
- Storage system configuration
- Storage area network (SAN) management and direct attach storage (DAS)
- Fibre Channel, Serial Attached SCSI (SAS), Internet SCSI (iSCSI), and Ethernet protocols

Related documentation

In addition to this guide, please refer to online help and the following documents for this product:

Related documentation

For information about	See
Enhancements, known issues, and late-breaking information not included in product documentation	Release Notes
Overview of product shipkit contents and setup tasks	Getting Started*
Regulatory compliance and safety and disposal information	AssuredSAN Product Regulatory Compliance and Safety*
Installing and using optional host-based software components (CAPI Proxy, MPIO DSM, VDS Provider, VSS Provider, SES Driver)	AssuredSAN Installing Optional Software for Microsoft Windows® Server
Recommendations for using optional data-protection features (AssuredSnap, AssuredCopy, AssuredRemote)	AssuredSAN 3000 Series Using Data Protection Software
Using a rackmount bracket kit to install an enclosure into a rack	AssuredSAN Rackmount Bracket Kit Installation* *or* AssuredSAN 2-Post Rackmount Bracket Kit Installation*
Product hardware setup and related troubleshooting	AssuredSAN 3000 Series Setup Guide
Obtaining and installing a license to use licensed features	AssuredSAN 3000 Series Obtaining and Installing a License Certificate File
Using the web interface to configure and manage the product	AssuredSAN 3000 Series RAIDar User Guide
Using the command-line interface (CLI) to configure and manage the product	AssuredSAN 3000 Series CLI Reference Guide
Event codes and recommended actions	AssuredSAN Event Descriptions Reference Guide
Identifying and installing or replacing field-replaceable units (FRUs)	AssuredSAN 3000 Series FRU Installation and Replacement Guide

* Printed document included in product shipkit.

For additional information, see Dot Hill's Customer Resource Center web site: http://crc.dothill.com.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text	Cross-reference links and e-mail addresses
Blue, underlined text	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

1 Getting started

RAIDar is a web-based application for configuring, monitoring, and managing the storage system.

Each controller module in the storage system contains a web server, which you access when you sign in to RAIDar. In a dual-controller system, you can access all functions from either controller. If one controller becomes unavailable, you can continue to manage the storage system from the partner controller.

RAIDar is also referred to as the web-browser interface (WBI).

Configuring and provisioning a new storage system

To configure and provision a storage system for the first time:

1. Configure your web browser for RAIDar and sign in, as described in Browser setup and Signing in below.
2. Set the system date and time, as described in Changing the system date and time on page 42.
3. Use the Configuration Wizard to configure other system settings, as described in Using the Configuration Wizard on page 33.
4. Use the Provisioning Wizard to create a virtual disk (*vdisk*) containing storage volumes, and optionally to map the volumes to hosts, as described in Using the Provisioning Wizard on page 55.
5. Use the Replication Setup Wizard to configure replication for a primary volume to a remote system, as described in Using the Replication Setup Wizard on page 110.
6. If you mapped volumes to hosts, verify the mappings by mounting/presenting the volumes from each host and performing simple read/write tests to the volumes.
7. Verify that controller modules and expansion modules have the latest firmware, as described in Viewing information about the system on page 87 and Updating firmware on page 75.

You can then make additional configuration and provisioning changes and view system status, as described in later chapters of this guide.

Browser setup

- Use Mozilla Firefox 3 or later, or Microsoft Internet Explorer 7 or later.
- To see the help window, you must enable pop-up windows.
- To optimize the display, use a color monitor and set its color quality to the highest setting.
- To navigate beyond the Sign In page (with a valid user account):
  - Set the browser's local-intranet security option to medium or medium-low. For Internet Explorer 8, adding each controller's network IP address as a trusted site can avoid access issues.
  - Verify that the browser is set to allow cookies at least for the IP addresses of the storage-system network ports.

Signing in

To sign in:

1. In the web browser's address field, type the IP address of a controller network port and press **Enter**. The RAIDar Sign In page is displayed. If the Sign In page does not display, verify that you have entered the correct IP address.
2. On the Sign In page, enter the name and password of a configured user. The default user name and password are `manage` and `!manage`. If you are logging in to RAIDar for the first time, the Language field displays `user setting` or `English`, either of which results in English.
3. Click **Sign In**. If the system is available, the System Overview page is displayed; otherwise, a message indicates that the system is unavailable.

Tips for signing in and signing out

- Do not include a leading zero in an IP address. For example, enter 10.1.4.6 not 10.1.4.**0**6.
- Multiple users can be signed in to each controller simultaneously.
- For each active RAIDar session an identifier is stored in the browser. Depending on how your browser treats this session identifier, you might be able to run multiple independent sessions simultaneously. Each instance of Internet Explorer can run a separate RAIDar session; however, all instances of Firefox share the same session.
- End a RAIDar session by clicking the Sign Out link near the top of the RAIDar window. Do not simply close the browser window.

Tips for using the main window

- The Configuration View panel displays logical and physical components of the storage system. To perform a task, select the component to act on and then either:
  - Right-click to display a context menu and select the task to perform. This is the method that help topics describe.
  - Click a task category in the main panel and select the task to perform.
- The System Status panel shows how many events of each severity have occurred in the system. To view event details, click a severity icon. For more information see Viewing the system event log on page 88.
- Many tables can be sorted by a specific column. To do so, click the column heading to sort low to high; click again to sort high to low. In tables that allow a task to be performed on multiple items, you can select up to 100 items or clear all selections by toggling the checkbox in the table's heading row.
- Do not use the browser's Back, Forward, Reload, or Refresh buttons. RAIDar has a single page whose content changes as you perform tasks and automatically updates to show current data.
- A red asterisk (*) identifies a required setting.
- The icon in the upper right corner of the main window shows the status of communication between RAIDar, the Management Controller (MC), and the Storage Controller (SC), as described in the following table.

Table 2 RAIDar communication status icons

Icon	Meaning
	RAIDar can communicate with the Management Controller, which can communicate with the Storage Controller.
	RAIDar *cannot* communicate with the Management Controller.
	RAIDar can communicate with the Management Controller, which *cannot* communicate with the Storage Controller.

- Below the communication status icon, a timer shows how long the session can be idle until you are automatically signed out. This timer resets after each action you perform. One minute before automatic sign-out you are prompted to continue using RAIDar.
- If a RAIDar session is active on a controller and the controller is power cycled or is forced offline by the partner controller or certain other events occur, the session might hang. RAIDar might say that it is "Connecting" but stop responding, or the page may become blank with the browser status "Done." After the controller comes back online, the session will not restart. To continue using RAIDar, close and reopen the browser and start a new RAIDar session.
- Colors that identify how storage space is used are described in About storage-space color codes on page 31.

- Icons shown in the Configuration View panel are described in About Configuration View icons on page 31.

Tips for using the help window

- To display help for a component in the Configuration View panel, right-click the component and select Help. To display help for the content in the main panel, click either Help in the menu bar or the help icon in the upper right corner of the panel.
- In the help window, click the table of contents icon to show or hide the Contents pane.
- As the context in the main panel is changed, the corresponding help topic is displayed in the help window. To prevent this automatic context-switching, click the pin icon. When a help window is pinned ( ), you can still browse to other topics within the help window and you can open a new help window. You cannot unpin a help window; you can only close it.
- If you have viewed more than one help topic, you can click the arrow icons to display the previous or next topic.

System concepts

About user accounts

The system provides three default user accounts and allows a maximum of 12 user accounts to be configured. Any account can be modified or removed except you cannot remove the user you are signed in as.

User accounts have these options:

- User Name. A user name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 29 bytes.
- Password. A password is case sensitive. A password cannot include a comma, double quote, or backslash.
- User Roles. Select Monitor to let the user view system settings, or Manage to let the user view and change system settings. You cannot change the roles of user `manage`.
- User Type. Select Standard to allow access to standard functions, or Advanced to allow access to all functions except diagnostic functions, or Diagnostic to allow access to all functions.

NOTE: This release has no functions that require Advanced or Diagnostic access; a Standard user can access all functions.

- WBI Access. Allows access to the web-based management interface.
- CLI Access. Allows access to the command-line management interface.
- FTP Access. Allows access to the file transfer protocol interface, which provides a way to install firmware updates and download logs.
- Base Preference. The base for entry and display of storage-space sizes. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.
- Precision Preference. The number of decimal places (1–10) for display of storage-space sizes.
- Unit Preference. Sets the unit for display of storage-space sizes. The Auto option lets the system determine the proper unit for a size. Based on the precision setting, if the selected unit is too large to meaningfully display a size, the system uses a smaller unit for that size. For example, if the unit is set to TB, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
- Temperature Preference. Specifies to use either the Celsius scale or the Fahrenheit scale for temperature values.
- Auto Sign Out. Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes). The default is 30 minutes.

- Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, and Spanish.

Table 3 Settings for default users

Name	Password	Roles	Type	WBI	CLI	FTP	Base	Prec.	Units	Temp.	Auto Sign Out	Locale
monitor	!monitor	Monitor	Standard	Yes	Yes	No	10	1	Auto	Celsius	30 Min.	English
manage	!manage	Monitor, Manage		Yes	Yes	Yes						
ftp	!ftp	Monitor, Manage		No	No	Yes						

NOTE: To secure the storage system, set a new password for each default user.

Related topics

- Configuring user accounts on page 40

About vdisks

A *vdisk* is a "virtual" disk that is composed of one or more disks, and has the combined capacity of those disks. The number of disks that a vdisk can contain is determined by its RAID level. All disks in a vdisk must be the same type (SAS or SATA, small or large form-factor). A maximum of 16 vdisks per controller can exist.

A vdisk can contain different models of disks, and disks with different capacities. For example, a vdisk can include a 500-GB disk and a 750-GB disk. If you mix disks with different capacities, the smallest disk determines the logical capacity of all other disks in the vdisk, regardless of RAID level. For example, if a RAID-0 vdisk contains one 500-GB disk and four 750-GB disks, the capacity of the vdisk is equivalent to approximately five 500-GB disks.

Each disk has metadata that identifies whether the disk is a member of a vdisk, and identifies other members of that vdisk. This enables disks to be moved to different slots in a system; an entire vdisk to be moved to a different system; and a vdisk to be quarantined if disks are detected missing.

In a single-controller system, all vdisks are owned by that controller. In a dual-controller system, when a vdisk is created the system automatically assigns the owner to balance the number of vdisks each controller owns; or, you can select the owner. Typically it does not matter which controller owns a vdisk.

In a dual-controller system, when a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources. If a fault-tolerant cabling configuration is used to connect the controllers to drive enclosures and hosts, both controllers' LUNs are accessible through the partner.

When you create a vdisk you can use the default chunk size or one that better suits your application. The chunk size is the amount of contiguous data that is written to a disk before moving to the next disk. After a vdisk is created its chunk size cannot be changed. For example, if the host is writing data in 16-KB transfers, that size would be a good choice for random transfers because one host read would generate the read of exactly one disk in the volume. That means if the requests are random-like, then the requests would be spread evenly over all of the disks, which is good for performance. If you have 16-KB accesses from the host and a 64-KB block size, then some of the hosts accesses would hit the same disk; each chunk contains four possible 16-KB groups of data that the host might want to read, which is not an optimal solution. Alternatively, if the host accesses were 128 KB, then each host read would have to access two disks in the vdisk. For random patterns, that ties up twice as many disks.

When you create a vdisk you can also create volumes within it. A volume is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. The storage system presents only volumes, not vdisks, to hosts.

You can create vdisks with or without volumes by using the Provisioning Wizard, or you can create vdisks manually.

Best practices for creating vdisks include:

- To maximize capacity, use disks of similar size.
- For greatest reliability, use disks of the same size and rotational speed.
- For storage configurations using many disks, create a few vdisks each containing many disks instead of many vdisks each containing a few disks.
- To maximize capacity and disk usage (but not performance), you can create vdisks larger than 2 TB and divide them into multiple volumes each having a capacity of 2 TB or less. This increases the usable capacity of storage configurations by reducing the total number of parity disks required when using parity-protected RAID levels. This differs from using a *volume* larger than 2 TB, which requires specific support by the host operating system, I/O adapter, and application.
- For maximum use of a dual-controller system's resources, each controller should own a similar number of vdisks.
- Set the chunk size to match the transfer block size of the host application.

Related topics

- About RAID levels on page 28
- About spares on page 19
- About volumes on page 20
- Vdisk topics in Provisioning the system on page 55
- Configuring a vdisk on page 50
- Verifying a vdisk on page 82
- Scrubbing a vdisk on page 82
- Viewing information about a vdisk (page 90), all vdisks (page 89), or the system (page 87)
- Removing a vdisk from quarantine on page 83

About spares

A controller automatically reconstructs a redundant (fault-tolerant) vdisk (RAID 1, 3, 5, 6, 10, 50) when one or more of its disks fails and a compatible spare disk is available. A compatible disk has enough capacity to replace the failed disk and is the same type (SAS or SATA).

There are three types of spares:

- *Dedicated spare*. Reserved for use by a specific vdisk to replace a failed disk. Most secure way to provide spares for vdisks but expensive to reserve a spare for each vdisk.
- *Global spare*. Reserved for use by any redundant vdisk to replace a failed disk.
- *Dynamic spare*. An available compatible disk that is automatically assigned to replace a failed disk in a redundant vdisk.

When a disk fails, the system looks for a dedicated spare first. If it does not find a dedicated spare, it looks for a global spare. If it does not find a compatible global spare and the dynamic spares option is enabled, it takes any available compatible disk. If no compatible disk is available, reconstruction cannot start.

A best practice is to designate spares for use if disks fail. Dedicating spares to vdisks is the most secure method, but it is also expensive to reserve spares for each vdisk. Alternatively, you can enable dynamic spares or assign global spares.

Related topics

- Configuring dynamic spares on page 45
- Managing dedicated spares on page 50
- Managing global spares on page 58
- Using the Provisioning Wizard on page 55
- Creating a vdisk on page 57

- Viewing information about a vdisk (page 90) or all vdisks (page 89)

About volumes

A *volume* is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. A mapped volume provides the storage for a file system partition you create with your operating system or third-party tools. The storage system presents only volumes, not vdisks, to hosts. A vdisk can have a maximum of 128 volumes.

You can create a vdisk that has one volume or multiple volumes.

- Single-volume vdisks work well in environments that need one large, fault-tolerant storage space for data on one host. A large database accessed by users on a single host that is used only for that application is an example.
- Multiple-volume vdisks work well when you have very large disks and you want to make the most efficient use of disk space for fault tolerance (parity and spares). For example, you could create one 10-TB RAID-5 vdisk and dedicate one spare to the vdisk. This minimizes the amount of disk space allocated to parity and spares compared to the space required if you created five 2-TB RAID-5 vdisks. However, I/O to multiple volumes in the same vdisk can slow system performance.

When you create volumes you can specify their sizes. If the total size of a vdisk's volumes equals the size of the vdisk, you will not have any free space. Without free space, you cannot add or expand volumes. If you need to add or expand a volume in a vdisk without free space, you can delete a volume to create free space. Or, you can expand the vdisk and then either add a volume or expand a volume to use the new free space.

You can use a volume's default name or change it to identify the volume's purpose. For example, a volume used to store payroll information can be named Payroll.

You can create vdisks with volumes by using the Provisioning Wizard, or you can create volumes manually.

Related topics

- About vdisks on page 18
- About volume mapping on page 21
- About volume cache options on page 22
- Volume topics in Provisioning the system on page 55
- Changing a volume's name on page 52
- Changing a volume's cache settings on page 52
- Viewing information about a volume on page 92

About hosts

A *host* identifies an external port that the storage system is attached to. The external port may be a port in an I/O adapter (such as an FC HBA) in a server, or a port in a network switch.

The controllers automatically discover hosts that have sent an `inquiry` command or a `report luns` command to the storage system. Hosts typically do this when they boot up or rescan for devices. When the command from the host occurs, the system saves the host ID. The ID for an FC or SAS host is its WWPN. The ID for an iSCSI host is typically, but not limited to, its IQN. You can also manually create entries for hosts.

You can assign a name to a host to make it easy to recognize for volume mapping. A maximum of 64 names can be assigned.

The Configuration View panel lists hosts by name, or if they are unnamed, by ID.

A storage system with iSCSI ports can be protected from unauthorized access via iSCSI by enabling Challenge Handshake Authentication Protocol (CHAP). CHAP authentication occurs during an attempt by a host to login to the system. This authentication requires an identifier for the host and a shared secret between the host and the system. Optionally, the storage system can also be required to authenticate itself to the host; this is called mutual CHAP. Steps involved in enabling CHAP include:

- Decide on host node names (identifiers) and secrets. The host node name is typically, but not limited to, its IQN. A secret must have 12–16 characters.
- Define CHAP entries in the storage system. If the node name is a host name, then it may be useful to display the hosts that are known to the system.
- Enable CHAP on the storage system. Note that this applies to all iSCSI hosts, in order to avoid security exposures.
- Define the CHAP secret(s) in the host iSCSI initiator.
- Request host login to the storage system. The host should be displayable by the system, as well as the ports through which connections were made.

If it becomes necessary to add more hosts after CHAP is enabled, additional CHAP node names and secrets can be added. If a host attempts to login to the storage system, it will become visible to the system, even if the full login is not successful due to incompatible CHAP definitions. This information may be useful in configuring CHAP entries for new hosts. This information becomes visible when an iSCSI discovery session is established, because the storage system does not require discovery sessions to be authenticated.

Related topics

- Using the Configuration Wizard on page 33
- Changing host interface settings on page 42
- Adding a host on page 70
- Removing hosts on page 70
- Changing a host's name on page 70
- Changing host mappings on page 71
- Viewing information about a host (page 97) or all hosts (page 97)

About volume mapping

Each volume has default host-access settings that are set when the volume is created; these settings are called the *default mapping*. The default mapping applies to any host that has not been explicitly mapped using different settings. *Explicit mappings* for a volume override its default mapping.

Default mapping enables all attached hosts to see a volume using a specified LUN and access permissions set by the administrator. This means that when the volume is first created, all connected hosts can immediately access the volume using the advertised default mapping settings. This behavior is expected by some operating systems, such as Microsoft Windows, which can immediately discover the volume. The advantage of a default mapping is that all connected hosts can discover the volume with no additional work by the administrator. The disadvantage is that all connected hosts can discover the volume with no restrictions. Therefore, this process is not recommended for specialized volumes that require restricted access.

You can change a volume's default mapping, and create, modify, or delete explicit mappings. A mapping can specify read-write, read-only, or no access through one or more controller host ports to a volume. When a mapping specifies no access, the volume is *masked*. You can apply access privileges to one or more of the host ports on either controller. To maximize performance, map a volume to at least one host port on the controller that owns it. To sustain I/O in the event of controller failure, map to at least one host port on each controller.

For example, a payroll volume could be mapped with read-write access for the Human Resources host and be masked for all other hosts. An engineering volume could be mapped with read-write access for the Engineering host and read-only access for other departments' hosts.

A LUN identifies a mapped volume to a host. Both controllers share a set of LUNs, and any unused LUN can be assigned to a mapping; however, each LUN can only be used once per volume as its default LUN. For example, if LUN 5 is the default for Volume1, no other volume in the storage system can use LUN 5 as its default LUN. For explicit mappings, the rules differ: LUNs used in default mappings can be reused in explicit mappings for other volumes and other hosts.

TIP: When an explicit mapping is deleted, the volume's default mapping takes effect. Therefore, it is recommended to use the same LUN for explicit mappings as for the default mapping.

Volume mapping settings are stored in disk metadata. If enough of the disks used by a volume are moved into a different enclosure, the volume's vdisk can be reconstructed and the mapping data is preserved.

3000 Series storage-system models use Unified LUN Presentation (ULP), which can expose all LUNs through all host ports on both controllers. The interconnect information is managed in the controller firmware. ULP appears to the host as an active-active storage system where the host can choose any available path to access a LUN regardless of vdisk ownership. When ULP is in use, the system's operating/redundancy mode is shown as Active-Active ULP. ULP uses the T10 Technical Committee of INCITS Asymmetric Logical Unit Access (ALUA) extensions, in SPC-3, to negotiate paths with aware host systems. Unaware host systems see all paths as being equal.

Related topics

- Using the Provisioning Wizard on page 55
- Changing a volume's default mapping (page 62) or explicit mappings (page 63)
- Changing host mappings on page 71
- Viewing information about a volume (page 92), snapshot (page 94), host (page 97), or all hosts (page 97)

About volume cache options

You can set options that optimize reads and writes performed for each volume.

Using write-back or write-through caching

CAUTION: Only disable write-back caching if you fully understand how the host operating system, application, and adapter move data. If used incorrectly, you might hinder system performance.

You can change a volume's write-back cache setting. *Write-back* is a cache-writing strategy in which the controller receives the data to be written to disks, stores it in the memory buffer, and immediately sends the host operating system a signal that the write operation is complete, without waiting until the data is actually written to the disk. Write-back cache mirrors all of the data from one controller module cache to the other. Write-back cache improves the performance of write operations and the throughput of the controller.

When write-back cache is disabled, *write-through* becomes the cache-writing strategy. Using write-through cache, the controller writes the data to the disks before signaling the host operating system that the process is complete. Write-through cache has lower write operation and throughput performance than write-back, but it is the safer strategy, with minimum risk of data loss on power failure. However, write-through cache does not mirror the write data because the data is written to the disk before posting command completion and mirroring is not required. You can set conditions that cause the controller to change from write-back caching to write-through caching.

In both caching strategies, active-active failover of the controllers is enabled.

You can enable and disable the write-back cache for each volume. By default, volume write-back cache is enabled. Because controller cache is backed by super-capacitor technology, if the system loses power, data is not lost. For most applications, this is the correct setting.

If you are doing random access to this volume, leave the write-back cache enabled.

The best practice for a fault-tolerant configuration is to use write-back caching.

Optimizing read-ahead caching

△ **CAUTION:** Only change read-ahead cache settings if you fully understand how the host operating system, application, and adapter move data so that you can adjust the settings accordingly.

You can optimize a volume for sequential reads or streaming data by changing its read-ahead cache settings. Read ahead is triggered by two back-to-back accesses to consecutive LBA ranges, whether forward (increasing LBAs) or reverse (decreasing LBAs).

You can change the amount of data read in advance after two back-to-back reads are made. Increasing the read-ahead cache size can greatly improve performance for multiple sequential read streams; however, increasing read-ahead size will likely decrease random read performance.

- The Default option works well for most applications: it sets one chunk for the first access in a sequential read and one stripe for all subsequent accesses. The size of the chunk is based on the chunk size used when you created the vdisk (the default is 64 KB). Non-RAID and RAID-1 vdisks are considered to have a stripe size of 64 KB.
- Specific size options let you select an amount of data for all accesses.
- The Maximum option lets the controller dynamically calculate the maximum read-ahead cache size for the volume. For example, if a single volume exists, this setting enables the controller to use nearly half the memory for read-ahead cache.

  Only use Maximum when disk latencies must be absorbed by cache. For example, for read-intensive applications, you will want data that is most often read to be in cache so that the response to the read request is very fast; otherwise, the controller has to locate which disks the data is on, move it up to cache, and then send it to the host. Do not use Maximum if more than two volumes are owned by the controller on which the read-ahead setting is being made. If there are more than two volumes, there is contention on the cache as to which volume's read data should be held and which has the priority; each volume constantly overwrites the other volume's data in cache, which could result in taking a lot of the controller's processing power.
- The Disabled option turns off read-ahead cache. This is useful if the host is triggering read ahead for what are random accesses. This can happen if the host breaks up the random I/O into two smaller reads, triggering read ahead.

You can also change the optimization mode.

- The standard read-ahead caching mode works well for typical applications where accesses are a combination of sequential and random; this method is the default. For example, use this mode for transaction-based and database update applications that write small files in random order.
- For an application that is strictly sequential and requires extremely low latency, you can use Super Sequential mode. This mode makes more room for read-ahead data by allowing the controller to discard cache contents that have been accessed by the host. For example, use this mode for video playback and multimedia post-production video- and audio-editing applications that read and write large files in sequential order.

Related topics

- Changing a volume's cache settings on page 52
- Changing system cache settings on page 47
- Viewing information about a volume on page 92

About managing remote systems

You can add a management object to obtain information from a remote storage system. This allows a local system to track remote systems by their network-port IP addresses and cache their login credentials — the user name and password for a manage-level user on that system. The IP address can then be used in commands that need to interact with the remote system.

After a remote system has been added, you can check the connectivity of host ports in the local system to host ports in that remote system. A port in the local system can only link to ports with the same host interface, such as Fibre Channel (FC), in a remote system.

Communication between local and remote systems is an essential part of the remote replication feature.

Related topics

- Adding a remote system on page 50
- Deleting remote systems on page 50
- Viewing information about a remote system on page 103
- Checking links to a remote system on page 85
- About the AssuredRemote replication feature on page 105

About the Snapshot feature

Snapshot (AssuredSnap™) is a licensed feature that provides data protection by enabling you to create and save snapshots of a volume. Each snapshot preserves the source volume's data state at the point in time when the snapshot was created. Snapshots can be created manually or by using the task scheduler.

When the first snapshot is taken of a standard volume, the system automatically converts the volume into a *master volume* and reserves additional space for snapshot data. This reserved space, called a *snap pool*, stores pointers to the source volume's data. Each master volume has its own snap pool. The system treats a snapshot like any other volume; the snapshot can be mapped to hosts with read-only access, read-write access, or no access, depending on the snapshot's purpose. Any additional unique data written to a snapshot is also stored in the snap pool.

The following figure shows how the data state of a master volume is preserved in the snap pool by two snapshots taken at different points in time. The dotted line used for the snapshot borders indicates that snapshots are logical volumes, not physical volumes as are master volumes and snap pools.

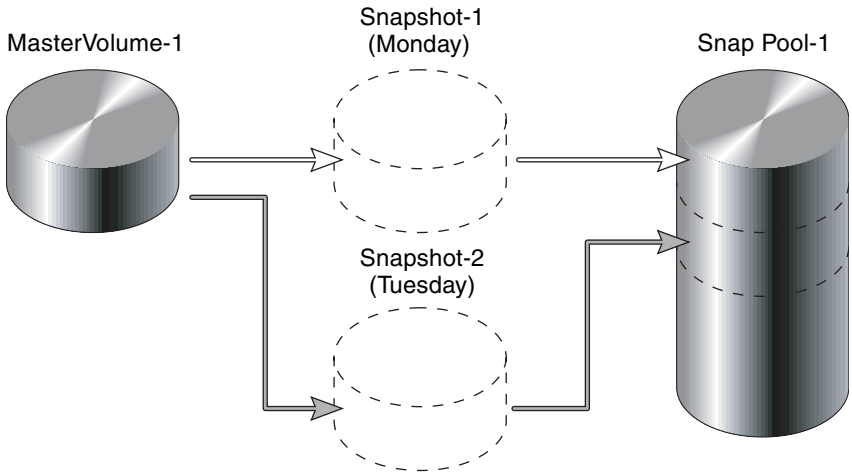


Figure 1 Relationship between a master volume and its snapshots and snap pool

The snapshot feature uses the single copy-on-write method to capture only data that has changed. That is, if a block is to be overwritten on the master volume, and a snapshot depends on the existing data in the block being overwritten, the data is copied from the master volume to the snap pool before the data is changed. All snapshots that depend on the older data are able to access it from the same location in the snap pool; this reduces the impact of snapshots when writing to a master volume. In addition, only a single copy-on-write operation is performed on the master volume.

The storage system allows a maximum number of snapshots to be retained, as determined by an installed license. For example, if your license allows four snapshots, when the fifth snapshot is taken an error message informs you that you have reached the maximum number of snapshots allowed on your system. Before you can create a new snapshot you must either delete an existing snapshot, or purchase and install a license that increases the maximum number of snapshots.

The snapshot service has two features for reverting data back to original data:

- Deleting only modified data on a snapshot. For snapshots that have been made accessible as read-write, you can delete just the modified (write) data that was written directly to a snapshot. When the modified data is deleted, the snapshot data reverts to the original data that was snapped. This feature is useful for testing an application, for example. You might want to test some code, which writes data to the snapshot. Rather than having to take another snapshot, you can just delete any write data and start again.
- Rolling back the data in a source volume. The rollback feature enables you to revert the data in a source volume to the data that existed when a specified snapshot was created (preserved data). Alternatively, the rollback can include data that has been modified (write data) on the snapshot since the snapshot was taken. For example, you might want to take a snapshot, mount/present/map that snapshot for read/write, and then install new software on that snapshot for test purposes. If the software installation is successful, you can rollback the master volume to the contents of the modified snapshot (preserved data plus the write data).

  The following figure shows the difference between rolling back the master volume to the data that existed when a specified snapshot was created (preserved), and rolling back preserved and modified data.

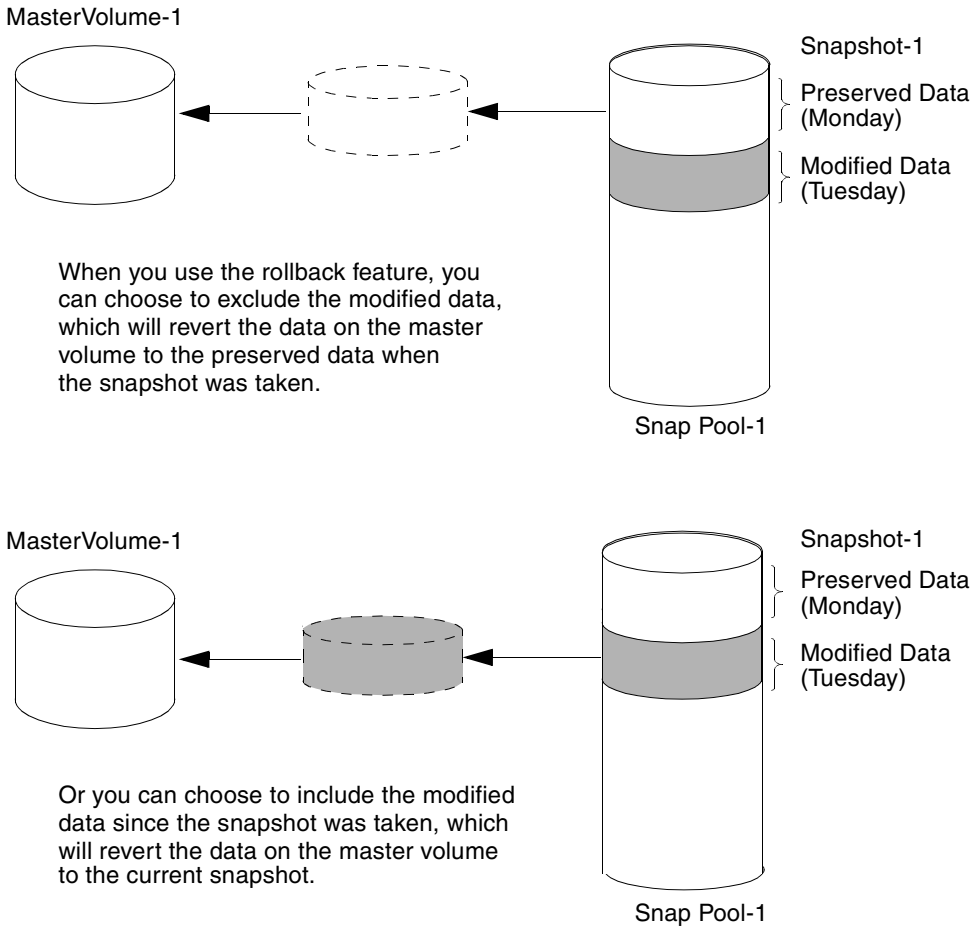

MasterVolume-1
Snapshot-1
Preserved Data
(Monday)
Modified Data
(Tuesday)
When you use the rollback feature, you can choose to exclude the modified data, which will revert the data on the master volume to the preserved data when the snapshot was taken.
Snap Pool-1
MasterVolume-1
Snapshot-1
Preserved Data
(Monday)
Modified Data
(Tuesday)
Or you can choose to include the modified data since the snapshot was taken, which will revert the data on the master volume to the current snapshot.
Snap Pool-1

Figure 2 Rolling back a master volume

Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

Related topics

- Installing a license on page 37
- Creating a snapshot (page 65) or multiple snapshots (page 64)
- Changing a snapshot's default mapping (page 62) or explicit mappings (page 63)
- Deleting snapshots on page 65
- Resetting a snapshot on page 66
- Viewing information about a snapshot (page 94), a vdisk (page 90), all vdisks (page 89), or the system (page 87)
- Rolling back a volume on page 68
- Deleting schedules on page 73

About the Volume Copy feature

Volume Copy (AssuredCopy™) is a licensed feature that enables you to copy a volume or a snapshot to a new standard volume.

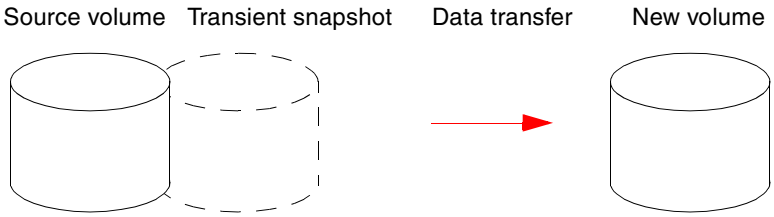
While a snapshot is a point-in-time logical copy of a volume, the volume copy service creates a complete "physical" copy of a volume within a storage system. It is an exact copy of a source volume as it existed at the time the volume copy operation was initiated, consumes the same amount of space as the source volume, and is independent from an I/O perspective. Volume independence is a key distinction of a volume copy (versus a snapshot, which is a "virtual" copy and dependent on the source volume).

Benefits include:

- Additional data protection. An independent copy of a volume (versus logical copy through snapshot) provides additional data protection against a complete master volume failure. If the source master volume fails, the volume copy can be used to restore the volume to the point in time the volume copy was taken.
- Non-disruptive use of production data. With an independent copy of the volume, resource contention and the potential performance impact on production volumes is mitigated. Data blocks between the source and the copied volumes are independent (versus shared with snapshot) so that I/O is to each set of blocks respectively; application I/O transactions are not competing with each other when accessing the same data blocks.

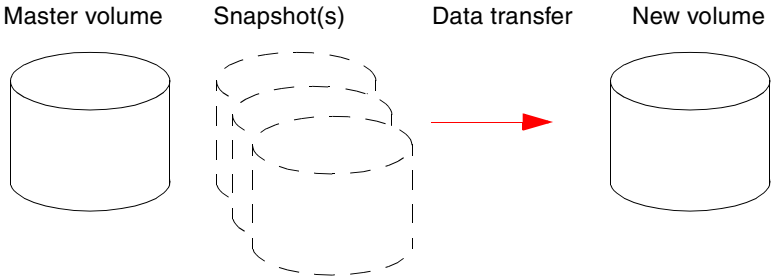
The following figure illustrates how volume copies are created.

Creating a volume copy from a standard or master volume



1. Volume copy request is made with a standard volume or a master volume as the source.
2. If the source a standard volume, it is converted to a master volume and a snap pool is created.
3. A new volume is created for the volume copy, and a hidden, transient snapshot is created.
4. Data is transferred from the transient snapshot to the new volume.
5. On completion, the transient volume is deleted and the new volume is a completely independent copy of the master volume, representing the data that was present when the volume copy was started.

Creating a volume copy from a snapshot



1. A master volume exists with one or more snapshots associated with it. Snapshots can be in their original state or they can be modified.
2. You can select any snapshot to copy, and you can specify that the modified or unmodified data be copied.
3. On completion, the new volume is a completely independent copy of the snapshot. The snapshot remains, though you can choose to delete it.

Figure 3 Creating a volume copy from a master volume or a snapshot

Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

Guidelines to keep in mind when performing a volume copy include:

- The destination vdisk must be owned by the same controller as the source volume.
- The destination vdisk must have free space that is at least as large as the amount of space allocated to the original volume. A new volume will be created using this free space for the volume copy.
- The destination vdisk does not need to have the same attributes (such as disk type, RAID level) as the volume being copied.
- Once the copy is complete, the new volume will no longer have any ties to the original.
- Volume Copy makes a copy from a snapshot of the source volume; therefore, the snap pool for the source volume must have sufficient space to store snapshot data when performing this copy.

Related topics

- Installing a license on page 37
- Creating a volume copy on page 67
- Aborting a volume copy on page 68
- Viewing information about a volume on page 92
- Deleting schedules on page 73

About the AssuredRemote replication feature

See page 105.

About the VDS and VSS hardware providers

Virtual Disk Service (VDS) enables host-based applications to manage vdisks and volumes. Volume Shadow Copy Service (VSS) enables host-based applications to manage snapshots. A license is required to enable VDS and VSS hardware providers, so hosts can manage vdisks, volumes, and snapshots in the storage system. For more information, see the VDS and VSS hardware provider documentation for your product.

About RAID levels

The RAID controllers enable you to set up and manage vdisks, whose storage may be spread across multiple disks. This is accomplished through firmware resident in the RAID controller. RAID refers to vdisks in which part of the storage capacity may be used to store redundant data. The redundant data enables the system to reconstruct data if a disk in the vdisk fails.

Hosts see each partition of a vdisk, known as a volume, as a single disk. A volume is actually a portion of the storage space on disks behind a RAID controller. The RAID controller firmware makes each volume appear as one very large disk. Depending on the RAID level used for a vdisk, the disk presented to hosts has advantages in fault-tolerance, cost, performance, or a combination of these.

NOTE: Choosing the right RAID level for your application improves performance.

The following tables:

- Provide examples of appropriate RAID levels for different applications
- Compare the features of different RAID levels
- Describe the expansion capability for different RAID levels

Table 4 Example applications and RAID levels

Application	RAID level
Testing multiple operating systems or software development (where redundancy is not an issue)	NRAID
Fast temporary storage or scratch disks for graphics, page layout, and image rendering	0
Workgroup servers	1 or 10
Video editing and production	3
Network operating system, databases, high availability applications, workgroup servers	5
Very large databases, web server, video on demand	50
Mission-critical environments that demand high availability and use large sequential workloads	6

Table 5 RAID level comparison

RAID level	Min. disks	Description	Strengths	Weaknesses
NRAID	1	Non-RAID, nonstriped mapping to a single disk	Ability to use a single disk to store additional data	Not protected, lower performance (not striped)
0	2	Data striping without redundancy	Highest performance	No data protection: if one disk fails all data is lost
1	2	Disk mirroring	Very high performance and data protection; minimal penalty on write performance; protects against single disk failure	High redundancy cost overhead: because all data is duplicated, twice the storage capacity is required
3	3	Block-level data striping with dedicated parity disk	Excellent performance for large, sequential data requests (fast read); protects against single disk failure	Not well-suited for transaction-oriented network applications: single parity disk does not support multiple, concurrent write requests
5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance and data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests; protects against single disk failure	Write performance is slower than RAID 0 or RAID 1
6	4	Block-level data striping with double distributed parity	Best suited for large sequential workloads; non-sequential read and sequential read/write performance is comparable to RAID 5; protects against dual disk failure	Higher redundancy cost than RAID 5 because the parity overhead is twice that of RAID 5; not well-suited for transaction-oriented network applications; non-sequential write performance is slower than RAID 5
10 (1+0)	4	Stripes data across multiple RAID-1 sub-vdisks	Highest performance and data protection (protects against multiple disk failures)	High redundancy cost overhead: because all data is duplicated, twice the storage capacity is required; requires minimum of four disks
50 (5+0)	6	Stripes data across multiple RAID-5 sub-vdisks	Better random read and write performance and data protection than RAID 5; supports more disks than RAID 5; protects against multiple disk failures	Lower storage capacity than RAID 5

Table 6 Vdisk expansion by RAID level

RAID level	Expansion capability	Maximum disks
NRAID	Cannot expand.	1
0, 3, 5, 6	You can add 1–4 disks at a time.	16
1	Cannot expand.	2
10	You can add 2 or 4 disks at a time.	16
50	You can add one sub-vdisk at a time. The added sub-vdisk must contain the same number of disks as each of the existing sub-vdisks.	32

About size representations

Parameters such as names of users and volumes have a maximum length in bytes. ASCII characters are 1 byte; most Latin (Western European) characters with diacritics are 2 bytes; most Asian characters are 3 bytes.

Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2. In RAIDar, the base for entry and display of storage-space sizes can be set per user or per session. When entering storage-space sizes only, either base-2 or base-10 units can be specified.

Table 7 Size representations in base 2 and base 10

Base 2		Base 10	
Unit	**Size in bytes**	**Unit**	**Size in bytes**
KiB (kibibyte)	1,024	KB (kilobyte)	1,000
MiB (mebibyte)	$1{,}024^2$	MB (megabyte)	$1{,}000^2$
GiB (gibibyte)	$1{,}024^3$	GB (gigabyte)	$1{,}000^3$
TiB (tebibyte)	$1{,}024^4$	TB (terabyte)	$1{,}000^4$
PiB (pebibyte)	$1{,}024^5$	PB (petabyte)	$1{,}000^5$
EiB (exbibyte)	$1{,}024^6$	EB (exabyte)	$1{,}000^6$

The locale setting determines the character used for the decimal (radix) point, as shown below.

Table 8 Decimal (radix) point character by locale

Language	Character	Examples
English, Chinese, Japanese, Korean	Period (.)	146.81 GB 3.0 Gb/s
Dutch, French, German, Italian, Spanish	Comma (,)	146,81 GB 3,0 Gb/s

Related topics

- About user accounts on page 17

About the system date and time

You can change the storage system's date and time, which are displayed in the System Status panel. It is important to set the date and time so that entries in system logs and event-notification email messages have correct time stamps.

You can set the date and time manually or configure the system to use Network Time Protocol (NTP) to obtain them from a network-attached server. When NTP is enabled, and if an NTP server is available, the system time and date can be obtained from the NTP server. This allows multiple storage devices, hosts, log files, and so forth to be synchronized. If NTP is enabled but no NTP server is present, the date and time are maintained as if NTP was not enabled.

NTP server time is provided in Coordinated Universal Time (UTC), which provides several options:

- If you want to synchronize the times and logs between storage devices installed in multiple time zones, set all the storage devices to use UTC.
- If you want to use the local time for a storage device, set its time zone offset.
- If a time server can provide local time rather than UTC, configure the storage devices to use that time server, with no further time adjustment.

Whether NTP is enabled or disabled, the storage system does not automatically make time adjustments, such as for U.S. daylight savings time. You must make such adjustments manually.

Related topics

- Changing the system date and time on page 42

About storage-space color codes

RAIDar panels use the following color codes to identify how storage space is used.

Table 9 Storage-space color codes

Area	Color	Meaning
Overview panels		Total space
		Available/free space
		Used space
		Reserved/overhead space, used for parity and snap pools, for example
Vdisk panels		Space used by spares
		Wasted space, due to use of mixed disk sizes

About Configuration View icons

The Configuration View panel uses the following icons to let you view physical and logical components of the storage system.

Table 10 Configuration View icons

Icon	Meaning	Icon	Meaning
	Show all subcomponents		Snapshot
	Hide all subcomponents		Snap pool
	Show the component's subcomponents		Replication-prepared volume
	Hide the component's subcomponents		Local primary volume
	Storage system		Local secondary volume
	Enclosure		Local replication image
	Host/initiator		Remote primary volume
	Vdisk		Remote secondary volume
	Standard or master volume		Remote replication image

About vdisk reconstruction

If one or more disks fail in a redundant vdisk (RAID 1, 3, 5, 6, 10, or 50) and compatible spares are available, the storage system automatically uses the spares to reconstruct the vdisk. Vdisk reconstruction does not require I/O to be stopped, so the vdisk can continue to be used while the Reconstruct utility runs.

A compatible spare is one whose capacity is equal to or greater than the smallest disk in the vdisk. A compatible spare has enough capacity to replace the failed disk and is the same type (SAS or SATA). If no compatible spares are available, reconstruction does not start automatically. To start reconstruction manually, replace each failed disk and then do one of the following:

- Add each new disk as either a dedicated spare or a global spare. Remember that a global spare might be taken by a different critical vdisk than the one you intended. When a global spare replaces a disk in a vdisk, the global spare's icon in the enclosure view changes to match the other disks in that vdisk.
- Enable the Dynamic Spare Capability option to use the new disks without designating them as spares.

RAID-6 reconstruction behaves as follows:

- If one disk fails and a compatible spare is available, the system begins to use that spare to reconstruct the vdisk. If a second disk fails during reconstruction, reconstruction continues until it is complete, regardless of whether a second spare is available. If the spare fails during reconstruction, reconstruction stops.
- If two disks fail and only one compatible spare is available, the system waits five minutes for a second spare to become available. After five minutes, the system begins to use that spare to reconstruct one disk in the vdisk (referred to as "fail 2, fix 1" mode). If the spare fails during reconstruction, reconstruction stops.
- If two disks fail and two compatible spares are available, the system uses both spares to reconstruct the vdisk. If one of the spares fails during reconstruction, reconstruction proceeds in "fail 2, fix 1" mode. If the second spare fails during reconstruction, reconstruction stops.
- If a disk fails during online initialization, the initialization fails. In order to generate the two sets of parity that RAID 6 requires, the controller fails a second disk in the vdisk, which changes the vdisk status to critical, and then assigns that disk as a spare for the vdisk. If a second spare is not available within five minutes, reconstruction proceeds in "fail 2, fix 1" mode.

When a disk fails, its fault LED illuminates amber. When a spare is used as a reconstruction target, its activity LED illuminates green.

NOTE: Reconstruction can take hours or days to complete, depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

About data protection in a single-controller storage system

A 3000 Series storage system can be purchased or operated with a single controller. Because single-controller mode is not a redundant configuration, this section presents some considerations concerning data protection.

A volume's default caching mode is write back, as opposed to write through. In write-back mode, data is held in controller cache until it is written to disk. In write-through mode, data is written directly to disk.

If the controller fails while in write-back mode, unwritten cache data likely exists. The same is true if the controller enclosure or the target volume's enclosure is powered off without a proper shut down. Data remains in the controller's cache and associated volumes will be missing that data. This can result in data loss or in some cases volume loss; for example, if using snapshot functionality a snap pool might become inaccessible and the master volume could go offline.

If the controller can be brought back online long enough to perform a proper shut down, the controller should be able to write its cache to disk without causing data loss.

To avoid the possibility of data loss in case the controller fails you can change a volume's caching mode to write through. While this will cause significant performance degradation, this configuration guards against data loss. While write-back mode is much faster, this mode is not guaranteed against data loss in the case of a controller failure. If data protection is more important, use write-through caching; if performance is more important, use write-back caching.

For details about caching modes see About volume cache options on page 22. To change a volume's caching mode, see Changing a volume's cache settings on page 52.

2 Configuring the system

Using the Configuration Wizard

The Configuration Wizard helps you initially configure the system or change system configuration settings.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Change passwords for the default users
- Configure each controller's network port
- Enable or disable system-management services
- Enter information to identify the system
- Configure event notification
- Configure controller host ports
- Confirm changes and apply them

When you complete this wizard you are given the option to start the Provisioning Wizard to provision storage.

Step 1: Starting the wizard

1. In the Configuration View panel, right-click the system and select either **Configuration > Configuration Wizard** or **Wizards > Configuration Wizard**. The wizard panel appears.
2. Click **Next** to continue.

Step 2: Changing default passwords

The system provides the default users `manage` and `monitor`. To secure the storage system, set a new password for each default user. A password is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 32 bytes.

Click **Next** to continue.

Step 3: Configuring network ports

You can configure addressing parameters for each controller's network port. You can set static IP values or use DHCP.

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one is available. If a DHCP server is unavailable, current addressing is unchanged. You must have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP server.

Each controller has the following factory-default IP settings:

- DHCP: disabled
- Controller A IP address: 10.0.0.2
- Controller B IP address: 10.0.0.3
- IP subnet mask: 255.255.255.0
- Gateway IP address: 10.0.0.1

When DHCP is enabled, the following initial values are set and remain set until the system is able to contact a DHCP server for new addresses:

- Controller IP addresses: 169.254.*x.x* (where the value of *x.x* is the lowest 16 bits of the controller serial number)
- IP subnet mask: 255.255.0.0
- Gateway IP address: 0.0.0.0

169.254.x.x addresses (including gateway 169.254.0.1) are on a private subnet that is reserved for unconfigured systems and the addresses are not routable. This prevents the DHCP server from reassigning the addresses and possibly causing a conflict where two controllers have the same IP address. As soon as possible, change these IP values to proper values for your network.

△ **CAUTION:** Changing IP settings can cause management hosts to lose access to the storage system.

To use DHCP to obtain IP values for network ports

1. Set IP address source to **DHCP**.
2. Click **Next** to continue.

To set static IP values for network ports

1. Determine the IP address, subnet mask, and gateway values to use for each controller.
2. Set IP address source to **manual**.
3. Set the values for each controller. You must set a unique IP address for each network port.
4. Click **Next** to continue.

Step 4: Enabling system-management services

You can enable or disable management-interface services to limit the ways in which users and host-based management applications can access the storage system. Network management interfaces operate out-of-band and do not affect host I/O to the system. The network options are:

- Web Browser Interface (WBI). The primary interface for managing the system. You can enable use of HTTP, of HTTPS for increased security, or both.
- Command Line Interface (CLI). An advanced user interface for managing the system. You can enable use of Telnet, of SSH (secure shell) for increased security, or both.
- Storage Management Initiative Spec. (SMIS). Used for remote management of the system through your network.

  The Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices.

  SMI-S replaces multiple disparate managed object models, protocols, and transports with a single object-oriented model for each type of component in a storage network. The specification was created by SNIA to standardize storage management solutions. SMI-S enables management applications to support storage devices from multiple vendors quickly and reliably because they are no longer proprietary. SMI-S detects and manages storage elements by type, not by vendor.
- File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
- Simple Network Management Protocol (SNMP). Used for remote monitoring of the system through your network.
- Service Debug. Used for technical support only.

In-band management interfaces operate through the data path and can slightly reduce I/O performance. The in-band option is:

- In-band SES Capability. Used for in-band monitoring of system status based on SCSI Enclosure Services (SES) data.

If a service is disabled, it continues to run but cannot be accessed. To allow specific users to access WBI, CLI, or FTP, see About user accounts on page 17.

To change management interface settings

1. Enable the options that you want to use to manage the storage system, and disable the others.
2. Click **Next** to continue.

Step 5: Setting system information

Enter a name, contact person, location, and description for the system. Each value can include a maximum of 79 bytes, using characters except double quote or backslash. The name is shown in the browser title bar or tab. The name, location, and contact are included in event notifications. All four values are recorded in system debug logs for reference by service personnel.

Click **Next** to continue.

Step 6: Configuring event notification

Configure up to four email addresses and three SNMP trap hosts to receive notifications of system events.

1. In the Email Configuration section, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: Critical (only); Error (and Critical); Warning (and Error and Critical); Informational (all). The default is none, which disables email notification.
   - SMTP Server address. The IP address of the SMTP mail server to use for the email messages. If the mail server is not on the local network, make sure that the gateway IP address was set in the network configuration step.
   - Sender Name. The sender name that is joined with an `@` symbol to the domain name to form the "from" address for remote notification. This name provides a way to identify the system that is sending the notification. The sender name can have a maximum of 31 bytes. Because this name is used as part of an email address, do not include spaces. For example: `Storage-1`. If no sender name is set, a default name is created.
   - Sender Domain. The domain name that is joined with an `@` symbol to the sender name to form the "from" address for remote notification. The domain name can have a maximum of 31 bytes. Because this name is used as part of an email address, do not include spaces. For example: `MyDomain.com`. If the domain name is not valid, some email servers will not process the mail.
   - Email Address fields. Up to four email addresses that the system should send notifications to. Email addresses must use the format *user-name@domain-name*. Each email address can have a maximum of 79 bytes. For example: `Admin@MyDomain.com`.
2. In the SNMP Configuration section, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: Critical (only); Error (and Critical); Warning (and Error and Critical); Informational (all). The default is none, which disables SNMP notification.
   - Read Community. The SNMP read password for your network. This password is also included in traps that are sent. The value is case sensitive; can include letters, numbers, hyphens, and underscores; and can have a maximum of 31 bytes. The default is `public`.
   - Write Community. The SNMP write password for your network. The value is case sensitive; can include letters, numbers, hyphens, and underscores; and can have a maximum of 31 bytes. The default is `private`.
   - Trap Host Address fields. IP addresses of up to three host systems that are configured to receive SNMP traps.
3. Click **Next** to continue.

Step 7: Configuring host ports

To enable the system to communicate with hosts or with remote systems, you must configure the system's host-interface options. There are options for FC and iSCSI ports but not for SAS ports.

For FC ports you can set these options:

- Speed can be set to auto (the default), which auto-negotiates the proper link speed with the host, or to 8Gb (Gbit per second), 4Gb, or 2Gb. Because a speed mismatch prevents communication between the port and host, set a speed only if you need to force the port to use a known speed for testing, or you need to specify a mutually supported speed for more than two FC devices connected in an arbitrated loop.

- Connection mode can be set to loop, point-to-point (the default for 3XX3 models), or auto (the default for 3XX0 models). Loop protocol can be used in a physical loop or in a direct physical connection between two devices. Point-to-point protocol can only be used on a direct physical connection between exactly two devices. Auto sets the mode based on the detected connection type.
- Loop IDs can be set, per controller, to use soft or hard target addressing:
  - Soft target addressing, which is the default, enables a LIP (loop initialization process) to determine the loop ID. Use this setting if the loop ID is permitted to change after a LIP or power cycle.
  - Hard target addressing requests a specific loop ID that should remain after a LIP or power cycle. If the port cannot acquire the specified ID, it is assigned a soft target address. Use this option if you want ports to have specific addresses, if your system checks addresses in reverse order (lowest address first), or if an application requires that specific IDs be assigned to recognize the controller.

For iSCSI ports you can set these options:

- IP Address. The port IP address.
- Netmask. The port netmask address.
- Gateway. The port gateway address.
- Authentication (CHAP). Enables or disables use of Challenge Handshake Authentication Protocol. Disabled by default.
- Jumbo Frames. Enables or disables support for jumbo frames. A normal frame can contain 1500 bytes whereas a jumbo frame can contain a maximum of 9000 bytes for larger data transfers. Disabled by default.

NOTE: Use of jumbo frames can succeed only if jumbo-frame support is enabled on all network components in the data path.

- Link Speed.
  - Auto: Auto-negotiates the proper speed. This is the default.
  - 1 Gbit/s: Forces the speed to 1 Gbit/sec, overriding a downshift that can occur during auto-negotiation with 1-Gbit/sec HBAs. This setting does not apply to 10-Gbit/sec HBAs.
- iSCSI IP Version. Specifies whether IP values use Internet Protocol version 4 (IPv4) or version 6 (IPv6) format. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.
- iSNS. Enables or disables registration with a specified Internet Storage Name Service server, which provides name-to-IP-address mapping. Disabled by default.
- iSNS Address. Specifies the IP address of an iSNS server. The default address is all zeroes.
- Alternate iSNS Address. Specifies the IP address of an alternate iSNS server, which can be on a different subnet. The default address is all zeroes.

For SAS ports there are no host-interface options. Click **Next** to continue.

To change FC host-interface settings

1. For controller host ports that are attached to hosts:
   - Set the speed to the proper value to communicate with the host.
   - Set the connection mode.
2. For each controller, set the loop ID to use soft or hard target addressing. To use soft target addressing, select **Soft?**. To use hard target addressing, clear **Soft?** and enter an address in the range 0–125. You cannot set the same hard target address for both controllers. An asterisk indicates that the value shown will be changed.
3. Click **Next** to continue.

To change iSCSI host-interface settings

1. For each iSCSI port, set the IP address, netmask, and gateway. Ensure that each iSCSI host port in the storage system is assigned a different IP address.
2. For all iSCSI ports, set the authentication, jumbo frames, link speed, and iSNS options.
3. Click **Next** to continue.

Step 8: Confirming configuration changes

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

NOTE: If you changed a controller's FC loop ID setting, you must restart the controller to make the change take effect.

Installing a license

A license is required to expand Snapshot limits and to use Volume Copy, Replication, VDS, and VSS. The license is specific to a controller enclosure serial number and firmware version.

If a permanent license is not installed and you want to try these features before buying a permanent license, you can create a temporary license one time. A temporary license will expire 60 days from the time it is created. After creating a temporary license, each time you sign in to RAIDar, a message specifies the time remaining in the trial period. If you do not install a permanent license before the temporary license expires, you cannot create new items with these features; however, you can continue to use existing items.

After a temporary license is created or a permanent license is installed, the option to create a temporary license is no longer displayed.

To view information about system licenses

In the Configuration View panel, right-click the system and select **Tools > Install License**.

The System Licenses table shows the following information about licensed features:

- Feature. The name of the licensed feature.
- Base. Either:
  - The number of components that users can create without a license.
  - N/A. Not applicable.
- License. Either:
  - The number of user-created components that the installed license supports.
  - Enabled or Disabled.
- In Use. Either:
  - The number of user-created components that exist.
  - N/A. Not applicable.
- Max Licensable. Either:
  - The number of user-created components that the maximum license supports.
  - N/A. Not applicable.
- Expiration. One of the following:
  - Never. License is purchased and doesn't expire.
  - Number of days remaining for a temporary license.
  - Expired. Temporary license has expired and cannot be renewed.
  - Expired/Renewable. Temporary license has expired and can be renewed.
  - N/A. No license installed.

The panel also shows the licensing serial number (controller enclosure serial number) and licensing version number (controller firmware version), for which a license file must be generated in order to successfully install.

To create a temporary license

1. In the Configuration View panel, right-click the system and select **Tools > Install License**. If the option to create a temporary license is available, the End User License Agreement appears in the lower portion of the license panel.
2. Read the license agreement.
3. If you accept the terms of the license agreement, select the checkbox. A confirmation dialog appears.
4. Click **Yes** to start the trial period. The feature's Expiration value shows the number of days remaining in the trial period; the trial period will expire on the last day. When the trial period expires, the value changes to Expired or Expired/Renewable.

To install a permanent license

1. Ensure that:
   - The license file is saved to a network location that RAIDar can access.
   - You are signed into the controller enclosure that the file was generated for.
2. In the Configuration View panel, right-click the system and select **Tools > Install License**.
3. Click **Browse** to locate and select the license file.
4. Click **Install License File**. If installation succeeds, the System Licenses table is updated. The licensing change takes effect immediately. The feature's Expiration value shows Never.

Configuring system services

Changing management interface settings

You can enable or disable management interfaces to limit the ways in which users and host-based management applications can access the storage system. Network management interfaces operate out-of-band and do not affect host I/O to the system. The network options are:

- Web Browser Interface (WBI). The primary interface for managing the system. You can enable use of HTTP, of HTTPS for increased security, or both.
- Command Line Interface (CLI). An advanced user interface for managing the system. You can enable use of Telnet, of SSH (secure shell) for increased security, or both.
- Storage Management Initiative Specification (SMIS). Used for remote management of the system through your network.
- File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
- Simple Network Management Protocol (SNMP). Used for remote monitoring of the system through your network.
- Service Debug. Used for technical support only.

In-band management interfaces operate through the data path and can slightly reduce I/O performance. The in-band option is:

- In-band SES Capability. Used for in-band monitoring of system status based on SCSI Enclosure Services (SES) data.

If a service is disabled, it continues to run but cannot be accessed. To allow specific users to access WBI, CLI, or FTP, see About user accounts on page 17.

To change management interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Management**.
2. Enable the options that you want to use to manage the storage system, and disable the others.
3. Click **Apply**. If you disabled any options, a confirmation dialog appears.
4. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
5. Click **OK**.

Configuring email notification

To configure email notification of events

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Email Notification**.
2. In the main panel, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: Critical (only); Error (and Critical); Warning (and Error and Critical); Informational (all). The default is none (Disabled), which disables email notification.
   - SMTP Server address. The IP address of the SMTP mail server to use for the email messages. If the mail server is not on the local network, make sure that the gateway IP address is set in System Settings > Network Interfaces.
   - Sender Name. The sender name that is joined with an `@` symbol to the domain name to form the "from" address for remote notification. This name provides a way to identify the system that is sending the notification. The sender name can have a maximum of 31 bytes. Because this name is used as part of an email address, do not include spaces. For example: `Storage-1`. If no sender name is set, a default name is created.
   - Sender Domain. The domain name that is joined with an `@` symbol to the sender name to form the "from" address for remote notification. The domain name can have a maximum of 31 bytes. Because this name is used as part of an email address, do not include spaces. For example: `MyDomain.com`. If the domain name is not valid, some email servers will not process the mail.
   - Email Address fields. Up to four email addresses that the system should send notifications to. Email addresses must use the format *user-name@domain-name*. Each email address can have a maximum of 79 bytes. For example: `Admin@MyDomain.com`.
3. Click **Apply**.
4. Optionally, send a test message to the configured destinations as described on page 81.

Configuring SNMP notification

To configure SNMP notification of events

1. In the Configuration View panel, right-click the system and select **Configuration > Services > SNMP Notification**.
2. In the main panel, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: Critical (only); Error (and Critical); Warning (and Error and Critical); Informational (all). The default is none, which disables SNMP notification.
   - Read Community. The SNMP read password for your network. This password is also included in traps that are sent. The value is case sensitive; can include any character except single quote and double quote; and can have a maximum of 31 bytes. The default is `public`.
   - Write Community. The SNMP write password for your network. The value is case sensitive; can include any character except single quote and double quote; and can have a maximum of 31 bytes. The default is `private`.
   - Trap Host Address fields. IP addresses of up to three host systems that are configured to receive SNMP traps.
3. Click **Apply**.
4. Optionally, send a test message to the configured destinations as described on page 81.

Configuring user accounts

Adding users

To add a user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Add User**.
2. In the main panel, set the options:
   - User Name. A user name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 29 bytes.

   NOTE: The user name `admin` is reserved for internal use.

   - Password. A password is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 32 bytes.
   - User Roles. Select Monitor to let the user view system settings, or Manage to let the user view and change system settings. You cannot change the roles of user `manage`.
   - User Type. Select Standard to allow access to standard functions, or Advanced to allow access to all functions except diagnostic functions, or Diagnostic to allow access to all functions.

   NOTE: This release has no functions that require Advanced or Diagnostic access; a Standard user can access all functions.

   - **WBI Access**. Allows access to the web-based management interface.
   - **CLI Access**. Allows access to the command-line management interface.
   - **FTP Access**. Allows access to the file transfer protocol interface, which provides a way to install firmware updates and download logs.
   - Base Preference. Select the base for entry and display of storage-space sizes. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.
   - Precision Preference. Select the number of decimal places (1–10) for display of storage-space sizes.
   - Unit Preference. Select the unit for display of storage-space sizes. Select Auto to let the system determine the proper unit for a size. Based on the precision setting, if the selected unit is too large to meaningfully display a size, the system uses a smaller unit for that size. For example, if the unit is set to TB, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
   - Temperature Preference. Specifies to use either the Celsius scale or the Fahrenheit scale for temperature values.
   - Auto Sign Out. Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes). The default is 30 minutes.
   - Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, and Spanish.
3. Click **Add User**.

Modifying users

To modify a user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Modify User**.
2. In the main panel, select the user to modify.
3. Set the options:
   - Password. A password is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 32 bytes.
   - User Roles. Select Monitor to let the user view system settings, or Manage to let the user view and change system settings. You cannot change the roles of user `manage`.
   - User Type. Select Standard to allow access to standard functions, or Advanced to allow access to all functions except diagnostic functions, or Diagnostic to allow access to all functions.

   NOTE: This release has no functions that require Advanced or Diagnostic access; a Standard user can access all functions.

   - **WBI Access**. Allows access to the web-based management interface.
   - **CLI Access**. Allows access to the command-line management interface.
   - **FTP Access**. Allows access to the file transfer protocol interface, which provides a way to install firmware updates and download logs.
   - Base Preference. Select the base for entry and display of storage-space sizes. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.
   - Precision Preference. Select the number of decimal places (1–10) for display of storage-space sizes.
   - Unit Preference. Select the unit for display of storage-space sizes. Select Auto to let the system determine the proper unit for a size. Based on the precision setting, if the selected unit is too large to meaningfully display a size, the system uses a smaller unit for that size. For example, if the unit is set to TB, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
   - Temperature Preference. Specifies to use either the Celsius scale or the Fahrenheit scale for temperature values.
   - Auto Sign Out. Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes). The default is 30 minutes.
   - Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, and Spanish.
4. Click **Modify User**.

   User changes take effect when the user next logs in.

Removing users

To remove a user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Remove User**.
2. In the main panel, select the user to remove. You cannot remove the `manage` user.
3. Click **Remove User**. A confirmation dialog appears.
4. Click **Remove** to continue; otherwise, click **Cancel**. If you clicked Remove, a processing dialog appears. When processing is complete, the user is removed from the table.
5. Click **OK**.

Configuring system settings

Changing the system date and time

You can enter values manually for the system date and time, or you can set the system to use NTP as explained in About the system date and time on page 30. Date and time values use Coordinated Universal Time (UTC).

To use manual date and time settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Date, Time**. The date and time options appear.
2. Set the options:
   - Time. Enter the time in the format *hh*:*mm*:*ss*, where *hh* is the hour (0–23), *mm* is the minutes (0–59), and *ss* is the seconds (0–59).
   - Month.
   - Day.
   - Year. Enter the year using four digits.
   - Network Time Protocol (NTP). Select **Disabled**.
3. Click **Apply**.

To obtain the date and time from an NTP server

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Date, Time**. The date and time options appear.
2. Set the options:
   - Network Time Protocol (NTP). Select **Enabled**.
   - NTP Time Zone Offset. Optional. The system's time zone as an offset in hours, and optionally minutes, from UTC. For example: the Pacific Time Zone offset is -8 during Pacific Standard Time or -7 during Pacific Daylight Time; the offset for Bangalore, India is +5:30.
   - NTP Server Address. Optional. If the system should retrieve time values from a specific NTP server, enter the address of an NTP server. If no IP server address is set, the system listens for time messages sent by an NTP server in broadcast mode.
3. Click **Apply**.

Changing host interface settings

To enable the system to communicate with hosts or with remote systems, you must configure the system's host-interface options. There are options for FC and iSCSI ports but not for SAS ports.

To change FC host interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
2. Set the speed to the proper value to communicate with the host. Speed can be set to auto (the default), which auto-negotiates the proper link speed with the host, or to 8Gb (Gbit per second), 4Gb, or 2Gb. Because a speed mismatch prevents communication between the port and host, set a speed only if you need to force the port to use a known speed for testing, or you need to specify a mutually supported speed for more than two FC devices connected in an arbitrated loop.
3. Set the connection mode to loop, point-to-point (the default for 3XX3 models), or auto (the default for 3XX0 models). Loop protocol can be used in a physical loop or in a direct physical connection between two devices. Point-to-point protocol can only be used on a direct physical connection between exactly two devices. Auto sets the mode based on the detected connection type.
4. Set the loop ID for each controller to request when the controller arbitrates during a LIP. A controller can use soft or hard target addressing:
   - Soft target addressing, which is the default, enables a LIP (loop initialization process) to determine the loop ID. Use this setting if the loop ID is permitted to change after a LIP or power cycle. To use this option, select **Soft?**.

- Hard target addressing requests a specific loop ID that should remain after a LIP or power cycle. If the port cannot acquire the specified ID, it is assigned a soft target address. Use this option if you want ports to have specific addresses, if your system checks addresses in reverse order (lowest address first), or if an application requires that specific IDs be assigned to recognize the controller. To use this option, clear **Soft** and enter an address in the range 0–125. You cannot set the same hard target address for both controllers.

5. Click **Apply**. If you changed a loop ID setting, a message specifies that you must restart the controller to make the change take effect. An asterisk indicates that the value shown will be changed.

To change iSCSI host interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
2. Set the port-specific options:
   - IP Address. For each controller, assign one port to one subnet and the other port to a second subnet. Ensure that each iSCSI host port in the storage system is assigned a different IP address. For example, in a system having only iSCSI ports:
     - Controller A port 0: 10.10.10.100
     - Controller A port 1: 10.11.10.120
     - Controller B port 0: 10.10.10.110
     - Controller B port 1: 10.11.10.130
   - Netmask. IP subnet mask. The default is 255.255.255.0.
   - Gateway. Gateway IP address. The default is 0.0.0.0.

   △ **CAUTION:** Changing IP settings can cause data hosts to lose access to the storage system.

3. Set the common options:
   - Authentication (CHAP). Enables or disables use of Challenge Handshake Authentication Protocol. Disabled by default.
   - Jumbo Frames. Enables or disables support for jumbo frames. A normal frame can contain 1500 bytes whereas a jumbo frame can contain a maximum of 9000 bytes for larger data transfers. Disabled by default.

   NOTE: Use of jumbo frames can succeed only if jumbo-frame support is enabled on all network components in the data path.

   - Link Speed.
     - Auto: Auto-negotiates the proper speed. This is the default.
     - 1 Gbit/s: Forces the speed to 1 Gbit/sec, overriding a downshift that can occur during auto-negotiation with 1-Gbit/sec HBAs. This setting does not apply to 10-Gbit/sec HBAs.
   - iSCSI IP Version. Specifies whether IP values use Internet Protocol version 4 (IPv4) or version 6 (IPv6) format. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.
   - iSNS. Enables or disables registration with a specified Internet Storage Name Service server, which provides name-to-IP-address mapping. Disabled by default.
   - iSNS Address. Specifies the IP address of an iSNS server. The default address is all zeroes.
   - Alternate iSNS Address. Specifies the IP address of an alternate iSNS server, which can be on a different subnet. The default address is all zeroes.
4. Click **Apply**.

Changing network interface settings

You can configure addressing parameters for each controller's network port. You can set static IP values or use DHCP.

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one is available. If a DHCP server is unavailable, current addressing is unchanged. You must have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP server.

Each controller has the following factory-default IP settings:

- DHCP: disabled
- Controller A IP address: 10.0.0.2
- Controller B IP address: 10.0.0.3
- IP subnet mask: 255.255.255.0
- Gateway IP address: 10.0.0.1

When DHCP is enabled, the following initial values are set and remain set until the system is able to contact a DHCP server for new addresses:

- Controller IP addresses: 169.254.*x.x* (where the value of *x.x* is the lowest 16 bits of the controller serial number)
- IP subnet mask: 255.255.0.0
- Gateway IP address: 0.0.0.0

169.254.*x.x* addresses (including gateway 169.254.0.1) are on a private subnet that is reserved for unconfigured systems and the addresses are not routable. This prevents the DHCP server from reassigning the addresses and possibly causing a conflict where two controllers have the same IP address. As soon as possible, change these IP values to proper values for your network.

△ **CAUTION:** Changing IP settings can cause management hosts to lose access to the storage system.

To use DHCP to obtain IP values for network ports

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Network Interfaces**.
2. Set the IP address source to **DHCP**.
3. Click **Apply**. If the controllers successfully obtain IP values from the DHCP server, the new IP values are displayed.
4. Record the new addresses.
5. Sign out and try to access RAIDar using the new IP addresses.

To set static IP values for network ports

1. Determine the IP address, subnet mask, and gateway values to use for each controller.
2. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Network Interfaces**.
3. Set the IP address source to manual.
4. Set the options for each controller. You must set a unique IP address for each network port.
5. Record the IP values you assign.
6. Click **Apply**.
7. Sign out and try to access RAIDar using the new IP addresses.

Setting system information

To set system information

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > System Information**.
2. In the main panel, set the name, contact person or group, location, and other information about the system. Each value can include a maximum of 79 bytes, using characters except double quote or backslash. The name is shown in the browser title bar or tab. The name, location, and contact are included in event notifications. All four values are recorded in system debug logs for reference by service personnel.
3. Click **Apply**.

Configuring advanced settings

Changing disk settings

Configuring SMART

Self-Monitoring Analysis and Reporting Technology (SMART) provides data that enables you to monitor disks and analyze why a disk failed. When SMART is enabled, the system checks for SMART events one minute after a restart and every five minutes thereafter. SMART events are recorded in the event log.

To change the SMART setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings** > **Disk**.
2. Set **SMART Configuration** to either:
   - **Don't Modify**. Allows current disks to retain their individual SMART settings and does not change the setting for new disks added to the system.
   - **Enabled**. Enables SMART for all current disks after the next rescan and automatically enables SMART for new disks added to the system. This option is the default.
   - **Disabled**. Disables SMART for all current disks after the next rescan and automatically disables SMART for new disks added to the system.
3. Click **Apply**.

Configuring dynamic spares

The dynamic spares feature lets you use all of your disks in redundant vdisks without designating a disk as a spare. With dynamic spares enabled, if a disk fails and you replace it with a compatible disk, the storage system rescans the bus, finds the new disk, automatically designates it a spare, and starts reconstructing the vdisk. A compatible disk has enough capacity to replace the failed disk and is the same type (SAS or SATA). If a dedicated spare, global spare, or compatible available disk is already present, the dynamic spares feature uses that disk to start the reconstruction and the replacement disk can be used for another purpose.

To change the dynamic spares setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Disk**.
2. Either select (enable) or clear (disable) the **Dynamic Spare Capability** option.
3. Click **Apply**.

Configuring drive spin down for available disks and global spares

The drive spin down (DSD) feature monitors disk activity within system enclosures and spins down inactive disks. You can enable or disable DSD for available disks and global spares, and set the period of inactivity after which the vdisk's disks and dedicated spares automatically spin down.

To configure a time period to suspend and resume DSD for all disks, see Scheduling drive spin down for all disks on page 46. To configure DSD for a vdisk, see Configuring drive spin down for a vdisk on page 51.

DSD affects disk operations as follows:

- Spun-down disks are not polled for SMART events.
- Operations requiring access to disks may be delayed while the disks are spinning back up.

To configure DSD for available disks and global spares

1. In the Configuration View panel, right-click the local system and select **Configuration > Advanced Settings > Disk**.
2. Set the options:
   - Either select (enable) or clear (disable) the **Available and Spare Drive Spin Down Capability** option. If you are enabling DSD, a warning prompt appears; to use DSD, click **Yes**; to leave DSD disabled, click **No**.
   - Set the **Drive Spin Down Delay (minutes)**, which is the period of inactivity after which available disks and global spares automatically spin down, from 1–360 minutes. If DSD is enabled and no delay value is set, the default is 15 minutes. The value 0 disables DSD.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

Scheduling drive spin down for all disks

For all disks that are configured to use drive spin down (DSD), you can configure a time period to suspend and resume DSD so that disks remain spun-up during hours of frequent activity.

To configure DSD for a vdisk, see Configuring drive spin down for a vdisk on page 51. To configure DSD for available disks and global spares, see Configuring drive spin down for available disks and global spares on page 45.

DSD affects disk operations as follows:

- Spun-down disks are not polled for SMART events.
- Operations requiring access to disks may be delayed while the disks are spinning back up.
- If a suspend period is configured and it starts while a disk has started spinning down, the disk spins up again.

To schedule DSD for all disks

1. In the Configuration View panel, right-click the local system and select **Configuration > Advanced Settings > Disk**.
2. Set the options:
   - Select the **Drive Spin Down Suspend Period** option.
   - Set a time to suspend and a time to resume DSD. For each, enter hour and minutes values and select either AM, PM, or 24H (24-hour clock).
   - If you want the schedule to apply only Monday through Friday, select the **Exclude Weekend Days from Suspend Period** option.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

Configuring the EMP polling rate

You can change the interval at which the storage system polls each attached enclosure's EMP for status changes. Typically you can use the default setting.

- Increasing the interval might slightly improve processing efficiency, but changes in device status are communicated less frequently. For example, this increases the amount of time before LEDs are updated to reflect status changes.
- Decreasing the interval slightly decreases processing efficiency, but changes in device status are communicated more frequently. For example, this decreases the amount of time before LEDs are updated to reflect status changes.

To change the EMP polling rate

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Disk**.
2. Set the EMP Polling Rate interval. The default is 5 seconds.
3. Click **Apply**.

Changing system cache settings

Changing the synchronize-cache mode

You can control how the storage system handles the `SCSI SYNCHRONIZE CACHE` command. Typically you can use the default setting. However, if the system has performance problems or problems writing to databases or other applications, contact technical support to determine if you should change this option.

To change the synchronize-cache mode

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Set **Sync Cache Mode** to either:
   - **Immediate**. Good status is returned immediately and cache content is unchanged. This is the default.
   - **Flush to Disk**. Good status is returned only after all write-back data for the specified volume is flushed to disk.
3. Click **Apply**.

Changing the missing LUN response

Some operating systems do not look beyond LUN 0 if they do not find a LUN 0 or cannot handle noncontiguous LUNs. The Missing LUN Response option handles these situations by enabling the host drivers to continue probing for LUNs until they reach the LUN to which they have access.

This option controls the SCSI sense data returned for volumes that are not accessible because they don't exist or have been hidden through volume mapping (this does not apply to volumes of offline vdisks). Use the default value unless a service technician asks you to change it to work around a host driver problem.

To change the missing LUN response

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Set **Missing LUN Response** to either:
   - **Not Ready**. Sends a reply that there is a LUN where a gap has been created but that it's "not ready." Sense data returned is a Sense Key of `2h` and an ASC/ASCQ of `04/03`. This option is the default.
   - **Illegal Request**. Sends a reply that there is a LUN but that the request is "illegal." Sense data returned is a Sense Key of `5h` and an ASC/ASCQ of `25/00`.
3. Click **Apply**.

Controlling host access to the system's write-back cache setting

You can prevent hosts from using `SCSI MODE SELECT` commands to change the system's write-back cache setting. Some operating systems disable write cache. If host control of write-back cache is disabled, the host cannot modify the cache setting. The default is Disabled.

This option is useful in some environments where the host disables the system's write-back cache, resulting in degraded performance.

To change host access to the write-back cache setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Either select (enable) or clear (disable) the **Host Control of Write-Back Cache** option.
3. Click **Apply**.

Changing auto-write-through cache triggers and behaviors

You can set conditions that cause ("trigger") a controller to change the cache mode from write-back to write-through, as described in About volume cache options on page 22. You can also specify actions for the system to take when write-through caching is triggered.

To change auto-write-through cache triggers and behaviors

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. In the Auto-Write Through Cache Trigger Conditions section, either select (enable) or clear (disable) the options:
   - **Controller Failure**. Changes to write-through if a controller fails. Disabled by default.
   - **Cache Power**. Changes to write-through if cache backup power is not fully charged or fails. Enabled by default.
   - **CompactFlash**. Changes to write-through if CompactFlash memory is not detected during POST, fails during POST, or fails while the controller is under operation. Enabled by default.
   - **Power Supply Failure**. Changes to write-through if a power supply unit fails. Disabled by default.
   - **Fan Failure**. Changes to write-through if a cooling fan fails. Disabled by default.
   - **Overtemperature Failure**. Forces a controller shutdown if a temperature is detected that exceeds system threshold limits. Disabled by default.
3. In the Auto-Write Through Cache Behaviors section, either select (enable) or clear (disable) the options:
   - **Revert when Trigger Condition Clears**. Changes back to write-back caching after the trigger condition is cleared. Enabled by default.
   - **Notify Other Controller**. Notifies the partner controller that a trigger condition occurred. Enable this option to have the partner also change to write-through mode for better data protection. Disable this option to allow the partner continue using its current caching mode for better performance. Disabled by default.
4. Click **Apply**.

Configuring partner firmware update

In a dual-controller system in which partner firmware update is enabled, when you update firmware on one controller, the system automatically updates the partner controller. Disable partner firmware update only if requested by a service technician.

To change the partner firmware update setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Firmware**.
2. Either select (enable) or clear (disable) the **Partner Firmware Update** option.
3. Click **Apply**.

Configuring system utilities

Configuring background scrub for vdisks

You can enable or disable whether the system continuously analyzes disks in vdisks to detect, report, and store information about disk defects. Vdisk-level errors reported include: hard errors, media errors, and bad block replacements (BBRs). Disk-level errors reported include: metadata read errors, SMART events during scrub, bad blocks during scrub, and new disk defects during scrub. For RAID 3, 5, 6, and 50, the utility checks all parity blocks to find data-parity mismatches. For RAID 1 and 10, the utility compares the primary and secondary disks to find data inconsistencies. For NRAID and RAID 0, the utility checks for media errors.

You can use a vdisk while it is being scrubbed. Background vdisk scrub runs at background utility priority, which reduces to no activity if CPU usage is above a certain percentage or if I/O is occurring on the vdisk being scrubbed. A vdisk scrub may be in process on multiple vdisks at once. A new vdisk will first be scrubbed 20 minutes after creation. After a vdisk is scrubbed, scrub will start again after the interval specified by the Vdisk Scrub Interval option.

When a scrub is complete, an event with code 207 is logged that specifies whether errors were found. For details, see the Event Descriptions Reference Guide.

Enabling background vdisk scrub is recommended for both SATA and SAS disks.

TIP: If you choose to disable background vdisk scrub, you can still scrub a selected vdisk by using Media Scrub Vdisk (page 82).

To configure background scrub for vdisks

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Set the options:
   - Either select (enable) or clear (disable) the **Vdisk Scrub** option. This option is disabled by default.
   - Set the **Vdisk Scrub Interval**, which is the interval between background vdisk scrub finishing and starting again, from 1–360 hours; the default is 24 hours.
3. Click **Apply**.

Configuring background scrub for disks not in vdisks

You can enable or disable whether the system continuously analyzes disks that are not in vdisks to detect, report, and store information about disk defects. Errors reported include: metadata read errors, SMART events during scrub, bad blocks during scrub, and new disk defects during scrub. The interval between background disk scrub finishing and starting again is 24 hours.

Enabling background vdisk scrub is recommended for both SATA and SAS disks.

To configure background scrub for vdisks

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Either select (enable) or clear (disable) the **Disk Scrub** option. This option is disabled by default.
3. Click **Apply**.

Configuring utility priority

You can change the priority at which the Verify, Reconstruct, Expand, and Initialize utilities run when there are active I/O operations competing for the system's controllers.

To change the utility priority

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Set **Utility Priority** to either:
   - **High**. Use when your highest priority is to get the system back to a fully fault-tolerant state. This causes heavy I/O with the host to be slower than normal. This value is the default.
   - **Medium**. Use when you want to balance data streaming with data redundancy.
   - **Low**. Use when streaming data without interruption, such as for a web server, is more important than data redundancy. This enables a utility such as Reconstruct to run at a slower rate with minimal effect on host I/O.
3. Click **Apply**.

Configuring remote systems

Adding a remote system

You can add a management object to obtain information from a remote storage system. This allows a local system to track remote systems by their network-port IP addresses and cache their login credentials. The IP address can then be used in commands that need to interact with the remote system.

To add a remote system

1. In the Configuration View panel, either:
   - Right-click the local system and select **Configuration > Remote System > Add Remote System**.
   - Right-click a remote system and select **Configuration > Add Remote System**.
2. In the main panel set the options:
   - **IP address**. IP address of a network port on the remote system.
   - **User Name**. User name for a user that has Manage-level access on the remote system.
   - **Password**. Optional. Password for the specified user.
3. Click **Create Remote System**. If the task succeeds, the new remote system appears in the Configuration View panel.

Deleting remote systems

You can delete the management objects for remote systems.

After establishing replication to a remote system, if you choose to delete the remote system you can safely do so without affecting replications. However, because the remote system's name and IP address will no longer appear in user interfaces, record this information before deleting the remote system so that you can access it at a later time, such as to delete old replication images or for disaster recovery.

To delete remote systems

1. In the Configuration View panel, either:
   - Right-click the local system and select **Configuration > Remote System > Delete Remote System**.
   - Right-click a remote system and select **Configuration > Delete Remote System**.
2. In the main panel, select the remote systems to remove. To select or clear all items, toggle the checkbox in the heading row.
3. Click **Delete Remote System(s)**. A confirmation dialog appears.
4. Click **Delete** to continue; otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, the System Overview panel and a success dialog appear.
5. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

Configuring a vdisk

Managing dedicated spares

You can assign a maximum of four available disks to a redundant vdisk (RAID 1, 3, 5, 6, 10, 50) for use as spares by that vdisk only. A spare must be the same type (SAS or SATA, small or large form-factor) as other disks in the vdisk, and have sufficient capacity to replace the smallest disk in the vdisk.

If a disk in the vdisk fails, a dedicated spare is automatically used to reconstruct the vdisk. A redundant vdisk other than RAID-6 becomes Critical when one disk fails. A RAID-6 vdisk becomes Degraded when one disk fails and Critical when two disks fail. After the vdisk's parity or mirror data is completely written to the spare, the vdisk returns to fault-tolerant status. For RAID-50 vdisks, if more than one sub-vdisk becomes critical, reconstruction and use of assigned spares occur in the order sub-vdisks are numbered.

To change a vdisk's spares

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Manage Dedicated Spares**. The main panel shows information about the selected vdisk, its spares, and all disks in the system. Existing spares are labeled SPARE.
   - In the Disk Sets table, the number of white slots in the SPARE entry's Disks field shows how many spares you can add to the vdisk.
   - In the enclosure view or list, only existing spares and suitable available disks are selectable.
2. Select spares to remove, disks to add as spares, or both.
3. Click **Modify Spares**. If the task succeeds, the panel is updated to show which disks are now spares for the vdisk.

Changing a vdisk's name

To change a vdisk's name

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Modify Vdisk Name**. The main panel shows the vdisk's name.
2. Enter a new name. A vdisk name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Modify Name**. The new name appears in the Configuration View panel.

Changing a vdisk's owner

Each vdisk is owned by one of the controllers, A or B, known as the *preferred owner*. Typically, you should not need to change vdisk ownership.

When a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources, becoming the *current owner*. If the system uses a fault-tolerant cabling configuration, both controllers' LUNs are accessible through the partner.

△ **CAUTION:**

- Before changing the owning controller for a vdisk, you must stop host I/O to the vdisk's volumes.
- Because a volume and its snap pool must be in vdisks owned by the same controller, if an ownership change will cause volumes and their snap pools to be owned by different controllers, the volumes will not be able to access their snap pools.

Changing the owner of a vdisk does not affect the mappings volumes in that vdisk.

To change a vdisk's owner

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Modify Vdisk Owner**. The main panel shows the vdisk's owner.
2. Select a new owner.
3. Click **Modify Owner**. A confirmation dialog appears.
4. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
5. Click **OK**.

Configuring drive spin down for a vdisk

The drive spin down (DSD) feature monitors disk activity within system enclosures and spins down inactive disks. For a specific vdisk, you can enable or disable DSD and set the period of inactivity after which the vdisk's disks and dedicated spares automatically spin down.

To configure a time period to suspend and resume DSD for all vdisks, see Scheduling drive spin down for all disks on page 46. To configure DSD for available disks and global spares, see Configuring drive spin down for available disks and global spares on page 45.

DSD affects disk operations as follows:

- Spun-down disks are not polled for SMART events.
- Operations requiring access to disks may be delayed while the disks are spinning back up.
- If a suspend period is configured and it starts while a vdisk has started spinning down, the vdisk spins up again.

To configure DSD for a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Configure Vdisk Drive Spin Down**.
2. Set the options:
   - Either select (enable) or clear (disable) the **Enable Drive Spin Down option**.
   - Set the **Drive Spin Down Delay (minutes)**, which is the period of inactivity after which the vdisk's disks and dedicated spares automatically spin down, from 1–360 minutes. If DSD is enabled and no delay value is set, the default is 15 minutes. A value of 0 disables DSD.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

Configuring a volume

Changing a volume's name

To change a volume's name

1. In the Configuration View panel, right-click a volume and select **Configuration > Modify Volume Name**.
2. Enter a new name. A volume name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Modify Name**. The new name appears in the Configuration View panel.

Changing a volume's cache settings

△ **CAUTION:**

- Only disable write-back caching if you fully understand how the host operating system, application, and adapter move data. If used incorrectly, you might hinder system performance.
- Only change read-ahead cache settings if you fully understand how the host operating system, application, and adapter move data so that you can adjust the settings accordingly.

To change a volume's cache settings

1. In the Configuration View panel, right-click a volume and select **Configuration > Modify Volume Cache Settings**.
2. In the main panel, set the read-ahead cache options:
   - Write Policy. Select write-back or write-through. The default is write-back.
   - Write Optimization. Select Standard or Super Sequential. The default is Standard.
   - Read Ahead Size. Select Default, Disabled, Maximum, or a specific size (64, 128, 256, or 512 KB; 1, 2, 4, 8, 16, or 32 MB).
3. Click **Modify Cache Settings**.

Configuring a snapshot

Changing a snapshot's name

To change a snapshot's name

1. In the Configuration View panel, right-click a snapshot and select C**onfiguration > Modify Snapshot Name**.
2. Enter a new name. A snapshot name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Modify Name**. The new name appears in the Configuration View panel.

Configuring a snap pool

Changing a snap pool's name

To change a snap pool's name

1. In the Configuration View panel, right-click a snap pool and select **Configuration > Modify Snap Pool Name**.
2. Enter a new name. A snap pool name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Modify Name**. The new name appears in the Configuration View panel.

3 Provisioning the system

Using the Provisioning Wizard

The Provisioning Wizard helps you create a vdisk with volumes and to map the volumes to hosts. Before using this wizard, read documentation for your product to learn about vdisks, volumes, and mapping. Then plan the vdisks and volumes you want to create and the default mapping settings you want to use.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Specify a name and RAID level for the vdisk
- Select disks to use in the vdisk
- Specify the number and size of volumes to create in the vdisk
- Specify the default mapping for access to the volume by hosts
- Confirm changes and apply them

Step 1: Starting the wizard

1. In the Configuration View panel, right-click the system and select either **Provisioning > Provisioning Wizard** or **Wizards > Provisioning Wizard**. The wizard panel appears.
2. Click **Next** to continue.

Step 2: Specifying the vdisk name and RAID level

A *vdisk* is a "virtual" disk that is composed of one or more disks, and has the combined capacity of those disks. The number of disks that a vdisk can contain is determined by its RAID level. All disks in a vdisk must be the same type (SAS or SATA, small or large form-factor). A maximum of 16 vdisks per controller can exist.

A vdisk can contain different models of disks, and disks with different capacities. For example, a vdisk can include a 500-GB disk and a 750-GB disk. If you mix disks with different capacities, the smallest disk determines the logical capacity of all other disks in the vdisk, regardless of RAID level. For example, if a RAID-0 vdisk contains one 500-GB disk and four 750-GB disks, the capacity of the vdisk is equivalent to approximately five 500-GB disks. To maximize capacity, use disks of similar size. For greatest reliability, use disks of the same size and rotational speed.

In a single-controller system, all vdisks are owned by that controller. In a dual-controller system, when a vdisk is created the system automatically assigns the owner to balance the number of vdisks each controller owns; or, you can select the owner. Typically it doesn't matter which controller owns a vdisk.

In a dual-controller system, when a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources. If the system uses a fault-tolerant cabling configuration, both controllers' LUNs are accessible through the partner.

When you create a vdisk you can also create volumes within it. A volume is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. The storage system presents only volumes, not vdisks, to hosts.

To create a vdisk

1. Set the options:
   - Vdisk name. Optionally change the default name for the vdisk. A vdisk name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
   - Assign to. If the system is operating in Active-Active ULP mode, optionally select a controller to be the preferred owner for the vdisk. The default, Auto, automatically assigns the owner to load-balance vdisks between controllers. If the system is operating in Single Controller mode, the Assign to setting is ignored and the system automatically load-balances vdisks in anticipation of the

insertion of a second controller in the future.

- RAID Level. Select a RAID level for the vdisk.
- Number of sub-vdisks. For a RAID-10 or RAID-50 vdisk, optionally change the number of sub-vdisks that the vdisk should contain.
- Chunk size. For RAID 3, 5, 6, 10, or 50, optionally set the amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk. For RAID 50, this option sets the chunk size of each RAID-5 sub-vdisk. The chunk size of the RAID-50 vdisk is calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). For NRAID and RAID 1, chunk size has no meaning and is therefore disabled. The default size is `512k`.

2. Click **Next** to continue.

Step 3: Selecting disks

Select disks to include in the vdisk. The Disk Selection Sets table has one row for each sub-vdisk in a RAID-10 or RAID-50 vdisk, or a single row for a vdisk having another RAID level. The table also has a SPARE row where you can assign dedicated spares to the vdisk. In each row, the Disks field shows how many disks you can, and have, assigned. As you select disks, the table shows the amount of storage space in the vdisk. For descriptions of storage-space color codes, see About storage-space color codes on page 31.

The Enclosures Front View table shows all disks in all enclosures. The Graphical tab shows disk information graphically; the Tabular tab shows disk information in a table. Disks you select are highlighted and color-coded to match the rows in the Disk Selection Sets table. Based on the type of disk you select first (SAS or SATA), only available disks of that type become selectable; you cannot mix SAS and SATA disks in a vdisk.

To select disks and spares

1. Select disks to populate each vdisk row. When you have selected enough disks, a checkmark appears in the table's Complete field.
2. Optionally select up to four dedicated spares for the vdisk.
3. Click **Next** to continue.

Step 4: Defining volumes

A *volume* is a logical subdivision of a vdisk and can be mapped to controller host ports for access by hosts. A mapped volume provides the storage for a file system partition you create with your operating system or third-party tools. The storage system presents only volumes, not vdisks, to hosts.

You can create multiple volumes with the same base name, size, and default mapping settings. If you choose to define volumes in this step, you will define their mapping settings in the next step.

To define volumes

1. Set the options:
   - Specify the number of volumes to create. If you do not want to create volumes, enter **0**. After changing the value, press **Tab**.
   - Optionally change the volume size. The default size is the total space divided by the number of volumes.
   - Optionally change the base name for the volumes. A volume name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
2. Click **Next** to continue.

Step 5: Setting the default mapping

Specify *default mapping* settings to control whether and how hosts will be able to access the vdisk's volumes. These settings include:

- A logical unit number (LUN), used to identify a mapped volume to hosts. Both controllers share one set of LUNs. Each LUN can be assigned as the default LUN for only one volume in the storage system; for example, if LUN 5 is the default for Volume1, LUN5 cannot be the default LUN for any other volume.
- The level of access — read-write, read-only, or no access — that hosts will have to each volume. When a mapping specifies no access, the volume is *masked*.
- Controller host ports through which hosts will be able to access each volume. To maximize performance, it is recommended to map a volume to at least one host port on the controller that the volume's vdisk is assigned to. To sustain I/O in the event of controller failure, it is recommended to map to at least one host port on each controller.

After a volume is created you can change its default mapping, and create, modify, or delete explicit mappings. An *explicit mapping* overrides the volume's default mapping for a specific host.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To specify the default mapping

1. Select **Map**.
2. Set the base LUN for the volumes. If this LUN is available, it will be assigned to the first volume and the next available LUNs in sequence will be assigned to any remaining volumes.
3. In the enclosure view or list, select controller host ports through which attached hosts can access each volume.
4. Select the access level that hosts will have to each volume: **read-write**, **read-only**, or **no-access** (masked)
5. Click **Next** to continue.

Step 6: Confirming vdisk settings

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

Creating a vdisk

To create a vdisk

1. In the Configuration View panel, right-click the system or **Vdisks** and then select **Provisioning > Create Vdisk**.
2. In the main panel set the options:
   - Vdisk name. Optionally change the default name for the vdisk. A vdisk name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
   - Assign to. If the system is operating in Active-Active ULP mode, optionally select a controller to be the preferred owner for the vdisk. The default, Auto, automatically assigns the owner to load-balance vdisks between controllers. If the system is operating in Single Controller mode, the Assign to setting is ignored and the system automatically load-balances vdisks in anticipation of the insertion of a second controller in the future.
   - RAID Level. Select a RAID level for the vdisk.
   - Number of Sub-vdisks. For a RAID-10 or RAID-50 vdisk, optionally change the number of sub-vdisks that the vdisk should contain.

- Chunk size. For RAID 3, 5, 6, 10, or 50, optionally set the amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk. For RAID 50, this option sets the chunk size of each RAID-5 sub-vdisk. The chunk size of the RAID-50 vdisk is calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). For NRAID and RAID 1, chunk size has no meaning and is therefore disabled. The default size is `512k`.
- Online Initialization. If this option is enabled, you can use the vdisk while it is initializing but because the verify method is used to initialize the vdisk, initialization takes more time. If this option is disabled, you must wait for initialization to complete before using the vdisk, but initialization takes less time. Online initialization is fault tolerant.

3. Select disks to include in the vdisk. Only available disks have checkboxes. The number of disks you can select is determined by the RAID level, and is specified in the Disk Selection Sets table. When you have selected enough disks, a checkmark appears in the table's Complete field.
4. Click **Create Vdisk**. If the task succeeds, the new vdisk appears in the Configuration View panel.

Deleting vdisks

△ **CAUTION:** Deleting a vdisk removes all of its volumes and their data.

To delete vdisks

1. Verify that hosts are not accessing volumes in the vdisks that you want to delete.
2. In the Configuration View panel, either:
   - Right-click the system or **Vdisks** and then select **Provisioning > Delete Vdisks**.
   - Right-click a vdisk and select **Provisioning > Delete Vdisk**.
3. In the main panel, select the vdisks to delete. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
4. Click **Delete Vdisk(s)**. A confirmation dialog appears.
5. Click **Delete** to continue; otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

Managing global spares

You can designate a maximum of eight global spares for the system. If a disk in any redundant vdisk (RAID 1, 3, 5, 6, 10, 50) fails, a global spare is automatically used to reconstruct the vdisk. At least one vdisk must exist before you can add a global spare. A spare must have sufficient capacity to replace the smallest disk in an existing vdisk.

The vdisk remains in critical status until the parity or mirror data is completely written to the spare, at which time the vdisk returns to fault-tolerant status. For RAID-50 vdisks, if more than one sub-vdisk becomes critical, reconstruction and use of spares occur in the order sub-vdisks are numbered.

To change the system's global spares

1. In the Configuration View panel, right-click the system and select **Provisioning > Manage Global Spares**. The main panel shows information about available disks in the system. Existing spares are labeled GLOBAL SP.
   - In the Disk Sets table, the number of white slots in the Disks field shows how many spares you can add.
   - In the enclosure view or list, only existing global spares and suitable available disks are selectable.
2. Select spares to remove, disks to add as spares, or both.
3. Click **Modify Spares**. If the task succeeds, the panel is updated to show which disks are now global spares.

Creating a volume set

In a vdisk that has sufficient free space, you can create multiple volumes with the same base name and size. Optionally, you can specify a default mapping for the volumes; otherwise, they will be created unmapped.

To create a volume set

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Volume Set**.
2. In the main panel, set the options:
   - Volume Set Base-name. Optionally change the base name for the volumes. The volume names will consist of the base name and a number that increments from 000. If a name in the series is already in use, the next name in the series is assigned. For example, for a two-volume set starting with Volume000, if Volume001 already exists, the second volume is named Volume002. A base name is case sensitive; cannot already be used by another vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 16 bytes.
   - Total Volumes. Specify the number of volumes to create. Volumes are created up to the maximum number supported per vdisk.
   - Size. Optionally change the volume size. The default size is the total space divided by the number of volumes.
   - Map. Select this option to specify a default mapping for the volumes:
     - Access. Select the access level that hosts will have to the volumes.
     - LUN. If the access level is set to read-write or read-only, set a LUN for the first volume. The next available LUN is assigned to the next volume mapped through the same ports. If a LUN to be assigned to a volume is already in use, that volume and any subsequent volumes are not mapped.
     - In the enclosure view or list, select controller host ports through which attached hosts can access the volumes.
3. Click **Apply**. If the task succeeds, the new volumes appear in the Configuration View panel.

Creating a volume

You can add a volume to a vdisk that has sufficient free space, and define default mapping settings.

To create a volume in a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Volume**.
2. In the main panel, set the options:
   - Volume name. Optionally change the default name. A volume name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
   - Size. Optionally change the default size, which is all free space in the vdisk.
   - Enable Snapshots. If the system is licensed to use Snapshots and you want to create snapshots of this volume, select this option. This specifies to create the volume as a master volume instead of as a standard volume, and enables the Snap Pool and Replication Prepare options.
   - Snap Pool. Select either:
     - Standard Policy. This option creates a snap pool named `sp`*`volume-name`* whose size is either 20% of the volume size or the minimum snap-pool size, whichever is larger.
     - Reserve Size. Specify the size of the snap pool to create in the vdisk and associate with the new volume. The default size is either 20% of the volume size or the minimum snap-pool size, whichever is larger.
     - Attach Pool. Select an existing snap pool to associate with the new volume.
   - Replication Prepare. If the system is licensed to use remote replication and you want to use this volume as a secondary volume, select this option. Selecting this option disables the Map option.

- Map. Select this option to change the default mapping for the volume:
  - Access. Select the access level that hosts will have to the volume.
  - LUN. If the access level is set to read-write or read-only, set a LUN for the volume.
  - In the enclosure view or list, select controller host ports through which attached hosts can access the volume.

3. Click **Apply**. If the task succeeds, the new volume appears in the Configuration View panel. If you specified an option to create a snap pool, the new snap pool also appears in that panel.

Deleting volumes

You can use the Delete Volumes panel to delete standard and master volumes.

△ **CAUTION:** Deleting a volume removes its mappings and schedules and deletes its data.

To delete volumes

1. Verify that hosts are not accessing the volumes that you want to delete.
2. In the Configuration View panel, either:
   - Right-click the system or **Vdisks** or a vdisk and then select **Provisioning > Delete Volumes**.
   - Right-click a volume and select **Provisioning > Delete Volume**.
3. In the main panel, select the volumes to delete. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
4. Click **Delete Volume(s)**.
5. Click **Delete** to continue; otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

NOTE: The system might be unable to delete a large number of volumes in a single operation. If you specified to delete a large number of volumes, verify that all were deleted. If some of the specified volumes remain, repeat the deletion on those volumes.

Changing default mapping for multiple volumes

For all volumes in all vdisks or a selected vdisk, you can change the default access to those volumes by all hosts. When multiple volumes are selected, LUN values are sequentially assigned starting with a LUN value that you specify. For example, if the starting LUN value is 1 for 30 selected volumes, the first volume's mapping is assigned LUN 1 and so forth, and the last volume's mapping is assigned LUN 30. For LUN assignment to succeed, ensure that no value in the sequence is already in use. When specifying access through specific ports, the ports and host must be the same type (for example, FC).

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

NOTE: You cannot map the secondary volume of a replication set.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To change default mapping for multiple volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Map Volume Defaults**.
2. In the main panel, select the volumes to change. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
3. Select **Map**.
4. Either:
   - Map the volumes to all hosts by setting a starting LUN, selecting ports, and setting access to **read-only** or **read-write**.
   - Mask the volumes from all hosts by setting a starting LUN, selecting ports, and setting access to **no-access**. Setting the default mapping to **no-access** will result in the LUN mapping being removed.
5. Click **Apply**. A message specifies whether the change succeeded or failed.
6. Click **OK**.

Explicitly mapping multiple volumes

For all volumes in all vdisks or a selected vdisk, you can change access to those volumes by a specific host. When multiple volumes are selected, LUN values are sequentially assigned starting with a LUN value that you specify. For example, if the starting LUN value is 1 for 30 selected volumes, the first volume's mapping is assigned LUN 1 and so forth, and the last volume's mapping is assigned LUN 30. For LUN assignment to succeed, ensure that no value in the sequence is already in use. When specifying access through specific ports, the ports and host must be the same type (for example, FC).

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

NOTE: You cannot map the secondary volume of a replication set.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To explicitly map multiple volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Map Volumes**.
2. In the main panel, select the volumes to change. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
3. In the Maps for Selected Volumes table, select the host to change access for.
4. Select **Map**.

5. Either:
   - Map the volumes to the host by setting a starting LUN, selecting ports, and setting access to **read-only** or **read-write**.
   - Mask the volumes from the host by setting a starting LUN, selecting ports, and setting access to **no-access**.
6. Click **Apply**. A message specifies whether the change succeeded or failed.
7. Click **OK**.

Changing a volume's default mapping

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/map a volume before changing the volume's LUN.

NOTE: You cannot map the secondary volume of a replication set.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To view the default mapping

In the Configuration View panel, right-click a volume and select **Provisioning > Default Mapping**. The main panel shows the volume's default mapping:

- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, not-mapped.

To modify the default mapping

1. Select **Map**.
2. Set the LUN and select the ports and access type. Setting the default mapping to **no-access** will result in the LUN mapping being removed.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. Each mapping that uses the default settings is updated.

To delete the default mapping

1. Clear **Map**.
2. Click **Apply**. A message specifies whether the change succeeded or failed.
3. Click **OK**. Each mapping that uses the default settings is updated.

Changing a volume's explicit mappings

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/unmap a volume before changing the volume's LUN.

NOTE: You cannot map the secondary volume of a replication set.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To view volume mappings

In the Configuration View panel, right-click a volume and select **Provisioning > Explicit Mappings**. The main panel shows the following information about the volume's mappings:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Name. Host name.
- Ports. Controller host ports through which the host is mapped to the volume.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

To create an explicit mapping

1. In the Maps for Volume table, select a host.
2. Select **Map**.
3. Set the LUN and select the ports and access type.
4. Click **Apply**. A message specifies whether the change succeeded or failed.
5. Click **OK**. The mapping becomes Explicit with the new settings.

To modify an explicit mapping

1. In the Maps for Volume table, select the Explicit mapping to change.
2. Set the LUN and select the ports and access type.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping settings are updated.

To delete an explicit mapping

1. In the Maps for Volume table, select the Explicit mapping to delete.
2. Clear **Map**.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping returns to the Default mapping.

Unmapping volumes

You can delete all of the default and explicit mappings for multiple volumes.

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

To unmap volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Unmap Volumes**.
2. In the main panel, select the volumes to unmap. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
3. Click **Unmap Volume(s)**. A message specifies whether the change succeeded or failed.
4. Click **OK**. Default and explicit mappings are deleted and the volumes' access type changes to not-mapped.

Expanding a volume

You can expand a standard volume if its vdisk has free space and sufficient resources. Because volume expansion does not require I/O to be stopped, the volume can continue to be used during expansion.

NOTE: This command is not supported for master volumes.

To expand a volume

1. In the Configuration View panel, right-click a standard volume and select **Tools > Expand Volume**.
2. In the main panel, specify the amount of free space to add to the volume.
3. Click **Expand Volume**. If the specified value exceeds the amount of free space in the vdisk, a dialog lets you expand the volume to the limit of free space in the vdisk. If the task succeeds, the volume's size is updated in the Configuration View panel.

Creating multiple snapshots

If the system is licensed to use Snapshots, you can select multiple volumes and immediately create a snapshot of each volume.

NOTE: The first time a snapshot is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or the minimum snap-pool size, whichever is larger. Before creating or scheduling snapshots, verify that the vdisk has enough free space to contain the snap pool.

To create multiple snapshots

1. In the Configuration View panel, right-click the system or **Vdisks** or a vdisk and then select **Provisioning > Create Multiple Snapshots**.
2. In the main panel, select each volume to take a snapshot of. To select up to 100 items or clear all selections, toggle the checkbox in the heading row.
3. Click **Create Snapshots**. If the task succeeds, the snapshots appear in the Configuration View panel.

Creating a snapshot

If the system is licensed to use Snapshots, you can create a snapshot now or schedule the snapshot task.

NOTE: The first time a snapshot is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or the minimum snap-pool size, whichever is larger. Before creating or scheduling snapshots, verify that the vdisk has enough free space to contain the snap pool.

To create a snapshot now

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Snapshot**.
2. In the main panel, select **Now**.
3. Optionally change the default name for the snapshot. A snapshot name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
4. Click **Create Snapshot**. If the task succeeds, the snapshot appears in the Configuration View panel.

To schedule a create snapshot task

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Snapshot**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - Snapshot prefix. Optionally change the default prefix to identify snapshots created by this task. The prefix is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 14 bytes. Automatically created snapshots are named *prefix*_s*n*, where *n* starts at 001.
   - Snapshots to Retain. Select the number of snapshots to retain. When the task runs, the retention count is compared with the number of existing snapshots:
     - If the retention count has not been reached, the snapshot is created.
     - If the retention count has been reached, the volume's oldest snapshot is unmapped, reset, and renamed to the next name in the sequence.
   - Start Schedule. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
     - Date must use the format *yyyy-mm-dd*.
     - Time must use the format *hh*:*mm* followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.
   - Recurrence. Specify the interval at which the task should run. Set the interval to at least two minutes. For better performance if this task will run under heavy I/O conditions or on more than three volumes, set the retention count and the schedule interval to similar values; for example if the retention count is 10 then the interval should be set to 10 minutes. The default is 1 minute.
   - Time Constraint. Specify a time range within which the task should run.
   - Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date.
   - End Schedule. Specify when the task should stop running.
4. Click **Schedule Snapshots**. If processing succeeds, the schedule is saved and can be viewed in the overview panel for the volume or system.

Deleting snapshots

You can use the Delete Snapshots panel to delete standard and replication snapshots.

When you delete a snapshot, all data uniquely associated with that snapshot is deleted and associated space in the snap pool is freed for use. Snapshots can be deleted in any order, irrespective of the order in which they were created.

△ **CAUTION:** Deleting a snapshot removes its mappings and schedules and deletes its data.

△ **CAUTION:** If a replication snapshot's type is shown as a "sync point" for its replication set, consider carefully whether you want to delete that snapshot. If you delete the current sync point, then if a replication-set failure occurs, a prior sync point will be used. If you delete the only sync point then the next replication will require a full sync to be performed (*all* data to be re-replicated from the primary volume to a secondary volume).

To delete snapshots

1. Verify that hosts are not accessing the snapshots that you want to delete.
2. In the Configuration View panel, right-click either the system or a vdisk or a master volume or a primary volume or a secondary volume or a snapshot or a replication image and then select **Provisioning > Delete Snapshot**.
3. In the main panel, select the snapshots to delete.
4. Click **Delete Snapshot(s)**.
5. Click **OK** to continue; otherwise, click **Cancel**. If you clicked OK, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

Resetting a snapshot

If the system is licensed to use Snapshots, as an alternative to taking a new snapshot of a volume, you can replace the data in a snapshot with the current data in the source volume. The snapshot's name and mapping settings are not changed. The snapshot data is stored in the source volume's snap pool.

△ **CAUTION:** To avoid data corruption, before resetting a snapshot it must be unmounted/unpresented/unmapped from hosts.

You can reset a snapshot now or schedule the reset task.

To reset a snapshot now

1. Unmount/unpresent/unmap the snapshot from hosts.
2. In the Configuration View panel, right-click a snapshot and select **Provisioning > Reset Snapshot**.
3. In the main panel, select **Now**.
4. Click **Reset Snapshot**. A confirmation dialog appears.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
6. Click **OK**.
7. Optionally, remount/re-present/remap the snapshot.

To schedule a reset snapshot task

1. In the Configuration View panel, right-click a snapshot and select **Provisioning > Reset Snapshot**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - Start Schedule. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
     - Date must use the format *yyyy-mm-dd*.
     - Time must use the format *hh:mm* followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.

- Recurrence. Specify the interval at which the task should run. Set the interval to at least 2 minutes. The default is 1 minute.
- Time Constraint. Specify a time range within which the task should run.
- Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date.
- End Schedule. Specify when the task should stop running.

4. Click **Reset Snapshot**. If the task succeeded, the schedule is saved and can be viewed in the overview panel for the snapshot or system.
5. Make a reminder to unmount/unpresent/unmap the snapshot before the scheduled task runs.

Creating a volume copy

If the system is licensed to use Volume Copy, you can copy a volume or a snapshot to a new standard volume. The destination volume must be in a vdisk owned by the same controller as the source volume. If the source volume is a snapshot, you can choose whether to include its modified data (data written to the snapshot since it was created). The destination volume is completely independent of the source volume.

The first time a volume copy is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or the minimum snap-pool size, whichever is larger. Before creating or scheduling copies, verify that the vdisk has enough free space to contain the snap pool.

For a master volume, the volume copy creates a transient snapshot, copies the data from the snapshot, and deletes the snapshot when the copy is complete. For a snapshot, the volume copy is performed directly from the source; this source data may change if modified data is to be included in the copy and the snapshot is mounted/presented/mapped and I/O is occurring to it.

To ensure the integrity of a copy of a master volume, unmount/unpresent/unmap the volume or at minimum perform a system cache flush and refrain from writing to the volume. Since the system cache flush is not natively supported on all operating systems, it is recommended to unmount/unpresent/unmap temporarily. The volume copy is for all data on the disk at the time of the request, so if there is data in the operating-system cache, that will not be copied over. Unmounting/unpresenting/unmapping the volume forces the cache flush from the operating system. After the volume copy has started, it is safe to remount/re-present/remap the volume and/or resume I/O.

To ensure the integrity of a copy of a snapshot with modified data, unmount/unpresent/unmap the snapshot or perform a system cache flush. The snapshot will not be available for read or write access until the volume copy is complete. If modified write data is not to be included in the copy, then you may safely leave the snapshot mounted/presented. During a volume copy using snapshot modified data, the system takes the snapshot offline, as shown by the Snapshot Overview panel.

The volume copy's progress is shown in the Volume Overview panel.

You can create a volume copy now or schedule the copy task.

To create a volume copy now

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Volume Copy**.
2. In the main panel, select **Now**.
3. Set the options:
   - New Volume Name. Optionally change the default name for the destination volume. A volume name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
   - Residing On Vdisk. Optionally change the destination vdisk.
   - **With Modified Data**. If the source volume is a snapshot, select this option to include the snapshot's modified data in the copy. Otherwise, the copy will contain only the data that existed when the snapshot was created.
4. Click **Copy the Volume**. A confirmation dialog appears.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes and With Modified Data is selected and the snapshot has modified data, a second confirmation dialog appears.

6. Click **Yes** to continue; otherwise, click No. If you clicked Yes, the volume copy operation starts. While the operation is in progress, the destination volume is offline and its type is shown as "standard*". If you unmounted/unpresented/unmapped a snapshot to copy its modified data, *wait* until processing is complete before you remount/re-present/remap it. If the task succeeds, the destination volume's type becomes standard and the volume appears in the Configuration View panel.
7. Optionally map the volume to hosts.

To schedule a volume copy task

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Volume Copy**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - New Volume Prefix. Optionally change the default prefix to identify volumes created by this task. The prefix is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 14 bytes. Automatically created volumes are named *prefix_cn*, where *n* starts at 001.
   - Residing On Vdisk. Optionally change the destination vdisk.
   - **With Modified Data**. If the source volume is a snapshot, select this option to include the snapshot's modified data in the copy. Otherwise, the copy will contain only the data that existed when the snapshot was created.
   - Start Schedule. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
     - Date must use the format *yyyy-mm-dd*.
     - Time must use the format *hh:mm* followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.
   - Recurrence. Specify interval at which the the task should run. Set the interval to at least 2 minutes. The default is 1 minute.
   - Time Constraint. Specify a time range within which the task should run.
   - Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date.
   - End Schedule. Specify when the task should stop running.
4. Click **Schedule Volume Copy**. If the task succeeded, the schedule is saved and can be viewed in the overview panel for the volume or system.
5. If you will copy snapshot modified data, make a reminder to unmount/unpresent/remap the snapshot before the scheduled task runs.

Aborting a volume copy

If the system is licensed to use Volume Copy, you can cancel an in-progress volume copy operation. When the cancellation is complete, the destination volume is deleted.

To abort a volume copy

1. In the Configuration View panel, right-click the destination volume and then select **Provisioning > Abort Volume Copy**. The Volume Overview panel shows the operation's progress.
2. Click **Abort Volume Copy**. A message confirms that the operation has been aborted.
3. Click **OK**. The destination volume is removed from the Configuration View panel.

Rolling back a volume

You can roll back (revert) the data in a volume to the data that existed when a specified snapshot was created. You also have the option of including its modified data (data written to the snapshot since it was created). For example, you might want to take a snapshot, mount/present/map it for read/write, and then install new software on the snapshot for testing. If the software installation is successful, you can roll back the volume to the contents of the modified snapshot.

△ **CAUTION:**

- Before rolling back a volume you must unmount/unpresent/unmap it from data hosts to avoid data corruption. If you want to include snapshot modified data in the roll back, you must also unmount/unpresent/unmap the snapshot.
- Whenever you perform a roll back, the data that existed on the volume is replaced by the data on the snapshot; that is, all data on the volume written since the snapshot was taken is lost. As a precaution, take a snapshot of the volume before starting a roll back.

Only one roll back is allowed on the same volume at one time. Additional roll backs are queued until the current roll back is complete. However, after the roll back is requested, the volume is available for use as if the roll back has already completed.

During a roll back operation using snapshot modified data, the snapshot must be unmounted/unpresented /unmapped and cannot be accessed. Unmounting/unpresenting/unmapping the snapshot ensures that all data cached by the host is written to the snapshot; if unmounting/unpresenting/unmapping is not performed at the host level prior to starting the roll back, data may remain in host cache, and thus not be rolled back to the master volume. As a precaution against inadvertently accessing the snapshot, the system also takes the snapshot offline, as shown by the Snapshot Overview panel. The snapshot becomes inaccessible in order to prevent any data corruption to the master volume. The snapshot can be remounted/re-presented/remapped once the roll back is complete.

To roll back a volume

1. Unmount/unpresent/unmap the volume from hosts.
2. If the roll back will include snapshot modified data, unmount/unpresent/unmap the snapshot from hosts.
3. In the Configuration View panel, right-click a volume and select **Provisioning > Roll Back Volume**.
4. In the main panel, set the options:
   - For Volume.
   - From Snapshot Volume. Enter the name of the snapshot to roll back to.
   - **With Modified Data**. Select this option to include the snapshot's modified data in the roll back. Otherwise, the master volume will contain only the data that existed when the snapshot was created.
5. Click **Roll Back Volume**. The roll back starts. You can now remount/re-present/remap the volume.
6. When the roll back is complete, if you unmounted/unpresented/unmapped the snapshot you can remount/re-present/remap it.

Creating a snap pool

Before you can convert a standard volume to a master volume or create a master volume for snapshots, a snap pool must exist. A snap pool and its associated master volumes can be in different vdisks, but must be owned by the same controller.

To create a snap pool

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Snap Pool**.
2. In the main panel set the options:
   - Snap Pool Name. Optionally change the default name for the snap pool. A snap pool name is case sensitive; cannot already exist in the system; and can have a maximum of 20 bytes. A name cannot include a comma, double quote, or backslash.
   - Size. Optionally change the default size, which is all free space in the vdisk. The supported minimum size is 5.37 GB. The recommended minimum size is 6 GB.
3. Click **Create Snap Pool** If the task succeeds, the new snap pool appears in the Configuration View panel.

Deleting snap pools

Before you can delete a snap pool you must delete any associated snapshots, and either delete the associated master volume or convert the master volume to a standard volume.

To delete snap pools

1. Verify that no master volume or snapshots are associated with the snap pool.
2. In the Configuration View panel, either:
   - Right-click the local system or **Vdisks** or a vdisk and select **Provisioning > Delete Snap Pools**.
   - Right-click a snap pool and select **Provisioning > Delete Snap Pool**.
3. In the main panel, select the snap pools to delete.
4. Click **Delete Snap Pool(s)**.
5. Click **Delete** to continue; otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

Adding a host

To add a host

1. Determine the host's WWPN or IQN.
2. In the Configuration View panel, right-click the system or **Hosts** and then select **Provisioning > Add Host**.
3. In the main panel set the options:
   - Host ID (WWN/IQN). Enter the host's WWPN or IQN. A WWPN value can include a colon between each pair of digits but the colons will be discarded.
   - Host Name. Optionally change the default name to one that helps you easily identify the host; for example, FileServer_1. A host name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 15 bytes.
4. Click **Add Host**. If the task succeeds, the new host appears in the Configuration View panel.

Removing hosts

To remove hosts

1. Verify that the hosts you want to remove are not accessing volumes.
2. In the Configuration View panel, either:
   - Right-click the system or **Hosts** and then select **Provisioning > Remove Hosts**.
   - Right-click a host and select **Provisioning > Remove Host**.
3. In the main panel, select the hosts to remove. To select or clear all items, toggle the checkbox in the heading row.
4. Click **Remove Host(s)**. A confirmation dialog appears.
5. Click **Remove** to continue; otherwise, click **Cancel**. If you clicked Remove, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

Changing a host's name

To change a host's name

1. In the Configuration View panel, right-click a host and select **Provisioning > Rename Host**.
2. Enter a new name that helps you easily identify the host; for example, FileServer_1. A host name is case sensitive; cannot already exist in the system; cannot include a comma, double quote, or backslash; and can have a maximum of 15 bytes.
3. Click **Modify Name**.

Changing host mappings

For each volume that is mapped to the selected host, you can create, modify, and delete explicit mappings. To change a volume's default mapping, see Changing a volume's default mapping on page 62.

△ **CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/unmap a volume before changing the volume's LUN.

NOTE: You cannot map the secondary volume of a replication set.

NOTE: When mapping a volume to a host using the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

To view host mappings

In the Configuration View panel, right-click a host and select **Provisioning > Manage Host Mappings**. The main panel shows the following information about volumes mapped to the host:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Name. Volume name.
- Serial Number. Volume serial number.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

To create an explicit mapping

1. In the Maps for Host table, select the Default mapping to override.
2. Select **Map**.
3. Set the LUN and select the ports and access type.
4. Click **Apply**. A message specifies whether the change succeeded or failed.
5. Click **OK**. The mapping becomes Explicit with the new settings.

To modify an explicit mapping

1. In the Maps for Host table, select the Explicit mapping to change.
2. Set the LUN and select the ports and access type.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping settings are updated.

To delete an explicit mapping

1. In the Maps for Host table, select the Explicit mapping to delete.
2. Clear **Map**.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping returns to the Default mapping.

Configuring CHAP

For iSCSI, you can use Challenge-Handshake Authentication Protocol (CHAP) to perform authentication between the initiator and target of a login request.

To perform this identification, a database of CHAP entries must exist on each device. Each CHAP entry can specify one name-secret pair to authenticate the initiator only (one-way CHAP) or two pairs to authenticate both the initiator and the target (mutual CHAP). For a login request from an iSCSI host to a storage system, the host is the initiator and the storage system is the target.

To enable or disable CHAP for all iSCSI hosts, see Changing host interface settings on page 42.

To add or modify a CHAP entry

1. In the Configuration View panel, right-click **Hosts** or a specific host and then select **Provisioning > Configure CHAP**. If any CHAP entries exist, a table shows them by node name.
2. Optionally, select an entry whose name you want to change to create a new entry. The entry's values appear in the option fields.
3. Set the options:
   - Node Name (IQN). The initiator name, typically in IQN format.
   - Secret. The secret that the target uses to authenticate the initiator. The secret is case sensitive and can include 12–16 bytes.
   - Name, if mutual CHAP. Optional; for mutual CHAP only. Specifies the target name, typically in IQN format. The name is case sensitive, can include a maximum of 223 bytes, and must differ from the initiator name. To find a controller iSCSI port's IQN, select the controller enclosure, view the Enclosure Overview panel (page 98), select the Rear Graphical tab, select an iSCSI port, and view the Target ID field.
   - Secret, if mutual CHAP. Optional; for mutual CHAP only. Specifies the secret that the initiator uses to authenticate the target. The secret is case sensitive, can include 12–16 bytes, and must differ from the initiator secret. A storage system's secret is shared by both controllers.
4. Click **Add/Modify Entry**. If the task succeeds, the new or modified entry appears in the CHAP entries table.

To delete a CHAP entry

1. In the Configuration View panel, right-click **Hosts** or a specific host and then select **Provisioning > Configure CHAP**. If any CHAP entries exist, a table shows them by node name.
2. Select the entry to delete.
3. Click **Delete Entry**. If the task succeeds, the entry is removed from the CHAP entries table.

Modifying a schedule

To modify a schedule

1. In the Configuration View panel, right-click the system or a volume or a snapshot and select **Provisioning > Modify Schedule**.
2. In the main panel, select the schedule to modify.
3. Set the options:
   - Snapshot Prefix. Optionally change the default prefix to identify snapshots created by this task. The prefix is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 14 bytes. Automatically created snapshots are named *prefix*_s*n*, where *n* starts at 001.
   - Snapshots to Retain. Select the number of snapshots to retain. When the task runs, the retention count is compared with the number of existing snapshots:
     - If the retention count has not been reached, the snapshot is created.
     - If the retention count has been reached, the volume's oldest snapshot is unmapped, reset, and renamed to the next name in the sequence.
   - Start Schedule. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.

- Date must use the format *yyyy-mm-dd*.
- Time must use the format *hh:mm* followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.

- Recurrence. Specify interval at which the task should run. The default is 30 minutes for a replication task or 1 minute for other tasks.
  - For a snapshot schedule, set the interval to at least 2 minutes. For better performance if this task will run under heavy I/O conditions or on more than three volumes, set the retention count and the interval to similar values; for example if the retention count is 10 then set the interval to 10 minutes.
  - For a volume-copy or reset-snapshot schedule, set the interval to at least 2 minutes.
  - For a replication schedule, set the interval to at least 30 minutes.
- Time Constraint. Specify a time range within which the task should run.
- Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date.
- End Schedule. Specify when the task should stop running.

4. Click **Modify Schedule**.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
6. Click **OK**.

Deleting schedules

If a component has a scheduled task that you no longer want to occur, you can delete the schedule. When a component is deleted, its schedules are also deleted.

To delete task schedules

1. In the Configuration View panel, right-click the system or a volume or a snapshot and select **Provisioning > Delete Schedule**.
2. In the main panel, select the schedule to remove.
3. Click **Delete Schedule**. A confirmation dialog appears.
4. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a processing dialog appears. If the task succeeds, the schedules are removed from the table and from the Configuration View panel. When processing is complete a success dialog appears.
5. Click **OK**.

4 Using system tools

Updating firmware

You can view the current versions of firmware in controller modules, expansion modules (in drive enclosures), and disks, and install new versions.

TIP: To ensure success of an online update, select a period of low I/O activity. This helps the update complete as quickly as possible and avoids disruptions to host and applications due to timeouts. Attempting to update a storage system that is processing a large, I/O-intensive batch job will likely cause hosts to lose connectivity with the storage system.

NOTE: If a vdisk is quarantined, firmware update is not permitted due to the risk of losing unwritten data that remains in cache for the vdisk's volumes. Before you can update firmware, you must resolve the problem that is causing the vdisk to be quarantined, as described in Removing a vdisk from quarantine on page 83.

Updating controller-module firmware

A controller enclosure can contain one or two controller modules. In a dual-controller system, both controllers should run the same firmware version. Storage systems in a replication set must run the same firmware version. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

If you have a dual-controller system and the Partner Firmware Update (PFU) option is enabled, when you update one controller the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

Firmware update via RAIDar is supported from an earlier TS230 version only.

To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to vdisks before starting the firmware update.
3. Restart the Management Controller (MC) in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers. For the procedure, see Restarting or shutting down controllers on page 80.
4. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Controller Versions shows the currently installed versions.
5. Click **Browse** and select the firmware file to install.
6. Click **Install Controller-Module Firmware File**. A dialog box shows firmware-update progress.

   The process starts by validating the firmware file:

   - If the file is invalid, verify that you specified the correct firmware file. If you did, try downloading it again from the source location.
   - If the file is valid, the process continues.

   CAUTION: Do not perform a power cycle or controller restart during a firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

Firmware update typically takes 10 minutes for a controller having current CPLD firmware, or 20 minutes for a controller having downlevel CPLD firmware. If the controller enclosure has attached drive enclosures, allow additional time for each expansion module's enclosure management processor (EMP) to be updated. This typically takes 3 minutes for each EMP in a drive enclosure.

If the Storage Controller cannot be updated, the update operation is cancelled. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

When firmware update on the local controller is complete, users are automatically signed out and the Management Controller will restart. Until the restart is complete, the RAIDar Sign In page will say that the system is currently unavailable. When this message is cleared, you may sign in.

If PFU is enabled, allow 10–20 minutes for the partner controller to be updated.

7. Clear your web browser's cache, then sign in to RAIDar. If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

NOTE: After firmware update has completed on both controllers, if the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

Updating expansion-module firmware

A drive enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

Expansion-module firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion module by loading a firmware file obtained from the enclosure vendor.

To update expansion-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to vdisks before starting the firmware update.
3. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Versions of All Expansion Modules (EMPs) shows the currently installed versions.
4. Select the expansion modules to update.
5. Click **Browse** and select the firmware file to install.
6. Click **Install Expansion-Module Firmware File**. Messages show firmware-update progress.

△ **CAUTION:** Do not perform a power cycle or controller restart during the firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

It typically takes 3 minutes to update each EMP in a drive enclosure. Wait for a message that the code load has completed.

7. Verify that each updated expansion module has the correct firmware version.

Updating disk firmware

You can update disk firmware by loading a firmware file obtained from your reseller.

A dual-ported disk can be updated from either controller. A single-ported disk that is in a vdisk or is a dedicated spare for a vdisk must be updated from the controller that owns the vdisk. Attempting to update a single-ported disk from the non-owning controller will not cause any change to the disk.

NOTE: Disks of the same model in the storage system must have the same firmware revision.

To update disk firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. Check the disk manufacturer's documentation to determine whether disks must be power cycled after firmware update.
3. Stop I/O to the storage system. During the update all volumes will be temporarily inaccessible to hosts. If I/O is not stopped, mapped hosts will report I/O errors. Volume access is restored after the update completes.
4. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Versions (Revisions) of All Disk Drives shows the currently installed versions.
5. Select the disks to update.
6. Click **Install Disk Firmware File**.

   CAUTION: Do not power cycle enclosures or restart a controller during the firmware update. If the update is interrupted or there is a power failure, the disk might become inoperative. If this occurs, contact technical support.

   It typically takes several minutes for the firmware to load. Wait for a message that the update has completed.
7. If the updated disks must be power cycled:
   a. Shut down both controllers; see Restarting or shutting down controllers on page 80.
   b. Power cycle all enclosures as described in your product's setup guide.

   NOTE: If you loaded firmware to a Seagate 750-Gbyte Barracuda ES SATA drive, after spin-up it will be busy for about 50 seconds completing its update. Then it will be ready for host I/O.
8. Verify that each disk has the correct firmware revision.

Saving logs

To help service personnel diagnose a system problem, you might be asked to provide system log data. Using RAIDar, you can save log data to a compressed zip file. The file will contain the following data:

- Device status summary, which includes basic status and configuration data for the system
- Each controller's event log
- Each controller's debug log
- Each controller's boot log, which shows the startup sequence
- Critical error dumps from each controller, if critical errors have occurred
- CAPI traces from each controller

NOTE: The controllers share one memory buffer for gathering log data and for loading firmware. Do not try to perform more than one save-logs operation at a time, or to perform a firmware-update operation while performing a save-logs operation.

To save logs

1. In the Configuration View panel, right-click the system and select **Tools > Save Logs**.
2. In the main panel:
   a. Enter your name, email address, and phone number so support personnel will know who provided the log data.
   b. Enter comments, describing the problem and specifying the date and time when the problem occurred. This information helps service personnel when they analyze the log data. Comment text can be 500 bytes long.
3. Click **Save Logs**.

   NOTE: In Microsoft Internet Explorer if the download is blocked by a security bar, select its **Download File** option. If the download does not succeed the first time, return to the Save Logs panel and retry the save operation.

   Log data is collected, which takes several minutes.
4. When prompted to open or save the file, click **Save**.
   - If you are using Firefox and have a download directory set, the file `store.zip` is saved there.
   - Otherwise, you are prompted to specify the file location and name. The default file name is `store.zip`. Change the name to identify the system, controller, and date.

NOTE: Because the file is compressed, you must uncompress it before you can view the files it contains. To examine diagnostic data, first view `store_yyyy_mm_dd__hh_mm_ss.logs`.

Resetting a host port

Making a configuration or cabling change on a host might cause the storage system to stop accepting I/O requests from that host. For example, this problem can occur after moving host cables from one HBA to another on the host. To fix such a problem you might need to reset controller host ports (channels).

For a Fibre Channel host port configured to use FC-AL (loop) topology, a reset issues a loop initialization primitive (LIP). For iSCSI, resetting a port might reset other ports. For SAS, resetting a host port issues a `COMINIT/COMRESET` sequence and might reset other ports.

To reset a host port

1. In the Configuration View panel, right-click the system and select **Tools > Reset Host Port**.
2. Select the port to reset. For example, to reset controller A port 1, select **A1**.
3. Click **Reset Host Port**.

Rescanning disk channels

A rescan forces a rediscovery of disks and enclosures in the storage system. If both Storage Controllers are online and able to communicate with both expansion modules in each disk enclosure, rescan also reassigns the enclosure IDs of attached enclosures based on controller A's enclosure cabling order. A manual rescan may be needed after system power-up to display enclosures in the proper order. A manual rescan temporarily pauses all I/O processes, then resumes normal operation. It can take up to two minutes for the enclosure IDs to be corrected.

A manual rescan is not needed after inserting or removing disks; the controllers automatically detect these changes. When disks are inserted they are detected after a short delay, which allows the disks to spin up.

To rescan disk channels

1. Verify that both controllers are operating normally.
2. In the Configuration View panel, right-click the system and select **Tools > Rescan Disk Channels**.
3. Click **Rescan**.

Restoring system defaults

If the system is not working properly and you cannot determine why, you can restore its default configuration settings. You then can reconfigure the settings that are necessary to use the system.

To restore defaults, use the CLI's `restore defaults` command, as described in the CLI reference guide.

Clearing disk metadata

△ **CAUTION:**

- Only use this command when all vdisks are online and leftover disks exist. Improper use of this command may result in data loss.
- Do not use this command when a vdisk is offline and one or more leftover disks exist.

If you are uncertain whether to use this command, contact technical support for further assistance.

Each disk in a vdisk has metadata that identifies the owning vdisk, the other members of the vdisk, and the last time data was written to the vdisk. The following situations cause a disk to become a *leftover*:

- Vdisk members' timestamps do not match so the system designates members having an older timestamp as leftovers.
- A disk is not detected during a rescan, then is subsequently detected.

When a disk becomes a leftover, the following changes occur:

- The disk's health becomes Degraded and its How Used state becomes LEFTOVR.
- The disk is automatically excluded from the vdisk, causing the vdisk's health to become Degraded or Fault, depending on the RAID level.
- The disk's fault LED is illuminated amber.

If spares are available, and the health of the vdisk is Degraded, the vdisk will use them to start reconstruction. When reconstruction is complete, you can clear the leftover disk's metadata. Clearing the metadata will change the disk's health to OK and its How Used state to AVAIL, making the disk available for use in a new vdisk or as a spare.

If spares are not available to begin reconstruction, or reconstruction has not completed, keep the leftover disk so that you'll have an opportunity to recover its data.

This command clears metadata from leftover disks only. If you specify disks that are not leftovers, the disks are not changed.

To clear metadata from leftover disks

1. In the Configuration View panel, right-click the system and then select **Tools > Clear Disk Metadata**.
2. In the main panel, select leftover disks to clear metadata from.
3. Click **Clear Metadata**. When processing is complete a success dialog appears.
4. Click **OK**.

Restarting or shutting down controllers

You can restart the processors in a controller module when RAIDar informs you that you have changed a configuration setting that requires restarting or when the controller is not working properly. Shut down the processors in a controller module before you remove it from an enclosure, or before you power off its enclosure for maintenance, repair, or a move.

A restart can be performed on either the Storage Controller processor or the Management Controller processor. A shut down affects both processors.

Restarting

If you restart a Storage Controller, it attempts to shut down with a proper failover sequence, which includes stopping all I/O operations and flushing the write cache to disk, and then the controller restarts. The Management Controller is not restarted so it can provide status information to external interfaces.

If you restart a Management Controller, communication with it is lost until it successfully restarts. If the restart fails, the partner MC remains active with full ownership of operations and configuration information.

△ **CAUTION:** If you restart both controller modules, you and users lose access to the system and its data until the restart is complete.

To perform a restart

1. In the Configuration View panel, right-click the local system and select **Tools > Shut Down or Restart Controller**.
2. In the main panel, set the options:
   - Select the **Restart** operation.
   - Select the type of controller processor to restart.
   - Select whether to restart the processor in controller A, B, or both.
3. Click **Restart now**. A confirmation dialog appears.
4. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a second confirmation dialog appears.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a message describes restart activity.

NOTE: If an iSCSI port is connected to a Microsoft Windows host, the following event is recorded in the Windows event log: `A connection to the target was lost, but Initiator successfully reconnected to the target.`

Shutting down

Shutting down the Storage Controller in a controller module ensures that a proper failover sequence is used, which includes stopping all I/O operations and writing any data in write cache to disk. If the Storage Controller in both controller modules is shut down, hosts cannot access the system's data. Perform a shut down before removing a controller module or powering down the system.

△ **CAUTION:** You can continue to use the CLI when either or both Storage Controllers are shut down, but information shown might be invalid.

To perform a shut down

1. In the Configuration View panel, right-click the local system and select **Tools > Shut Down or Restart Controller**.
2. In the main panel, set the options:
   - Select the **Shut down** operation.
   - Select whether to restart the processor in controller A, B, or both.
3. Click **Shut down now**. A confirmation dialog appears.
4. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a second confirmation dialog appears.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, a message describes shutdown activity.

NOTE: If an iSCSI port is connected to a Microsoft Windows host, the following event is recorded in the Windows event log: `Initiator failed to connect to the target.`

Testing event notification

You can send a test message to verify that interfaces such as email, SNMP, and SMI-S that are configured to receive event-notification messages do receive them. Email and SNMP configuration settings must include a notification level other than "none (Disabled)" for event messages to be sent to those interfaces.

To send a test message

1. In the Configuration View panel, right-click the local system and select **Tools > Send Test Notification**.
2. Click **Send**. If the task succeeds, verify that the test message reached the destinations.

Expanding a vdisk

You can expand the capacity of a vdisk by adding disks to it, up to the maximum number of disks that the storage system supports. Host I/O to the vdisk can continue while the expansion proceeds. You can then create or expand a volume to use the new free space, which becomes available when the expansion is complete. You can expand only one vdisk at a time. The RAID level determines whether the vdisk can be expanded and the maximum number of disks the vdisk can have.

IMPORTANT: Expansion can take hours or days to complete, depending on the vdisk's RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop expansion only by deleting the vdisk.

Before expanding a vdisk

Back up the vdisk's data so that if you need to stop expansion and delete the vdisk, you can move the data into a new, larger vdisk.

To expand a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Tools > Expand Vdisk**. Information appears about the selected vdisk and all disks in the system.
   - In the Disk Selection Sets table, the number of white slots in the vdisk's Disks field shows how many disks you can add to the vdisk.
   - In the enclosure view or list, only suitable available disks are selectable.
2. Select disks to add.
3. Click **Expand Vdisk**. A processing dialog appears.
4. Click **OK**. The expansion's progress is shown in the **View > Overview** panel.

Verifying a vdisk

If you suspect that a redundant (mirror or parity) vdisk has a problem, you can run the Verify utility to check the vdisk's integrity. For example, if the storage system was operating outside the normal temperature range, you might want to verify its vdisks. The Verify utility checks whether the redundancy data in the vdisk is consistent with the user data in the vdisk. For RAID 3, 5, 6, and 50, the utility checks all parity blocks to find data-parity mismatches. For RAID 1 and 10, the utility compares the primary and secondary disks to find data inconsistencies.

Verification can last over an hour, depending on the size of the vdisk, the utility priority, and the amount of I/O activity. When verification is complete, the number of inconsistencies found is reported with event code 21 in the event log. Such inconsistencies can indicate that a disk in the vdisk is going bad. For information about identifying a failing disk, use the SMART option (see Configuring SMART on page 45). You can use a vdisk while it is being verified.

If too many utilities are running for verification to start, either wait until those utilities have completed and try again, or abort a utility to free system resources. If you abort verification, you cannot resume it; you must start it over.

To verify a vdisk

1. In the Configuration View panel, right-click a redundant vdisk and select **Tools > Verify Vdisk**.
2. Click **Start Verify Utility**. A message confirms that verification has started.
3. Click **OK**. The panel shows the verification's progress.

To abort vdisk verification

1. In the Configuration View panel, right-click a redundant vdisk and select **Tools > Verify Vdisk**.
2. Click **Abort Verify Utility**. A message confirms that verification has been aborted.
3. Click **OK**.

Scrubbing a vdisk

The system-level Vdisk Scrub option (see Configuring background scrub for vdisks on page 48) automatically checks all vdisks for disk defects. If this option is disabled, you can still perform a scrub on a selected vdisk.

The scrub utility analyzes a vdisk to detect, report, and store information about disk defects. Vdisk-level errors reported include: hard errors, media errors, and bad block replacements (BBRs). Disk-level errors reported include: metadata read errors, SMART events during scrub, bad blocks during scrub, and new disk defects during scrub. For RAID 3, 5, 6, and 50, the utility checks all parity blocks to find data-parity mismatches. For RAID 1 and 10, the utility compares the primary and secondary disks to find data inconsistencies. For NRAID and RAID 0, the utility checks for media errors. This utility does not fix defects.

You can use a vdisk while it is being scrubbed. A scrub can last over an hour, depending on the size of the vdisk, the utility priority, and the amount of I/O activity. However, a "foreground" scrub performed by Media Scrub Vdisk is typically faster than a background scrub performed by Vdisk Scrub.

When a scrub is complete, an event with code 207 is logged that specifies whether errors were found. For details, see the Event Descriptions Reference Guide.

To scrub a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Tools > Media Scrub Vdisk**.
2. Click **Start Media Scrub Utility**. A message confirms that the scrub has started.
3. Click **OK**. The panel shows the scrub's progress.

To abort a vdisk scrub

1. In the Configuration View panel, right-click a vdisk and select **Tools > Media Scrub Vdisk**.

NOTE: If the vdisk is being scrubbed but the Abort Media Scrub Utility button is grayed out, a background scrub is in progress. To stop the background scrub, disable the Vdisk Scrub option as described in Configuring background scrub for vdisks on page 48.

---

2. Click **Abort Media Scrub Utility**. A message confirms that the scrub has been aborted.
3. Click **OK**.

Removing a vdisk from quarantine

A vdisk having a fault-tolerant RAID level becomes quarantined if at least one of its disks is detected as missing after the storage system is powered up or while it is operating. Quarantine does not occur for NRAID or RAID-0 vdisks; if known-failed disks are missing; or if disks are missing after failover or recovery.

Quarantine isolates the vdisk from host access, and prevents the system from changing the vdisk status to OFFL (offline). The number of missing disks determines the quarantine status; from least to most severe:

- QTDN: Quarantined with down disks. At least one disk is missing; however, the vdisk could be accessed and would be fault tolerant. For instance, one disk is missing from a RAID-6.
- QTCR: Quarantined critical. At least one disk is missing; however, the vdisk could be accessed. For instance, one disk is missing from a mirror or RAID-5.
- QTOF: Quarantined offline. Multiple disks are missing and user data is incomplete.

When a vdisk is quarantined, its disks are write-locked, its volumes become inaccessible, and it is not available to hosts until it is dequarantined. If there are interdependencies between the quarantined vdisk's volumes and volumes in other vdisks, quarantine may temporarily impact operation of those other volumes. For example, if the quarantined vdisk contains the snap pool used for snapshot, volume-copy, or replication operations, quarantine may temporarily cause the associated master volume to go offline; a volume-copy or replication operation can also be disrupted if an associated volume (snap pool, source volume, or destination volume) goes offline. Depending on the operation, the length of the outage, and the settings associated with the operation, the operation may resume automatically resume when the vdisk is dequarantined or may require manual intervention. A vdisk can remain quarantined indefinitely without risk of data loss.

Examples of when quarantine might occur are:

- At system power-up, a vdisk has fewer disks online than at the previous power-up. This may happen because a disk is slow to spin up, or because a drive enclosure is not powered up. The vdisk will be automatically dequarantined if the missing disks come online and the vdisk status becomes FTOL (fault tolerant and online), or if after 60 seconds the vdisk status is QTCR or QTDN.
- A vdisk that is not running I/O loses redundancy plus one more disk. The vdisk will be automatically dequarantined if the missing disks come online and the vdisk status becomes FTOL, or if after 60 seconds the vdisk status is QTCR or QTDN.
- A vdisk running I/O loses redundancy plus one more disk. The vdisk will be automatically dequarantined if the vdisk's status is QTCR or QTDN.

A vdisk is dequarantined when it is brought back online, which can occur in three ways:

- If the missing disks come online, making the vdisk FTOL, the vdisk is automatically dequarantined.
- If after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined. The missing disks are marked as failed and the vdisk status changes to CRIT (critical) or FTDN (fault tolerant with down disks).

- Dequarantine Vdisk is used to manually dequarantine the vdisk. If the missing disks later come online, they are marked as LEFTOVR (leftover).

A quarantined vdisk can be fully recovered if the missing disks are restored. Make sure that all disks are properly seated, that no disks have been inadvertently removed, and that no cables have been unplugged. Sometimes not all disks in the vdisk power up. Check that all enclosures have restarted after a power failure. If these problems are found and then fixed, the vdisk recovers and no data is lost.

If the missing disks cannot be restored (for example, they failed), you can dequarantine the vdisk to restore operation in some cases. If you dequarantine a vdisk that is not missing too many disks, its status changes to CRIT. Then, if spares of the appropriate size are available, reconstruction begins.

If a replacement disk (reconstruct target) is missing on power up, the vdisk becomes quarantined; when the disk is found, the vdisk is dequarantined and reconstruction starts. If reconstruction was in process, it continues where it left off.

NOTE: The only tasks allowed for a quarantined vdisk are Dequarantine Vdisk and Delete Vdisk. If you delete a quarantined vdisk and its missing disks later come online, the vdisk will reappear as quarantined or offline and you must delete it again (to clear those disks).

CAUTION: If the vdisk does not have enough disks to continue operation, when the vdisk is removed from quarantine its status changes to OFFL and its data cannot be recovered. To continue operation, a RAID-3 or RAID-5 vdisk can be missing one disk; a RAID-6 vdisk can be missing one or two disks; a RAID-10 or RAID-50 vdisk can be missing one disk per sub-vdisk. For example, a 16-disk RAID-10 vdisk can remain online (critical) with 8 disks missing if one disk per mirror is missing.

To remove a vdisk from quarantine

1. In the Configuration View panel, right-click a quarantined vdisk and select **Tools > Dequarantine Vdisk**.
2. Click **Dequarantine Vdisk**. Depending on the number of disks that remain active in the vdisk, its health might change to Degraded (RAID 6 only) and its status changes to FTOL, CRIT, or FTDN. For status descriptions, see Vdisk properties on page 90.

Expanding a snap pool

By default, snap pools are configured to automatically expand when they become 90% full.

However, if a snap pool's policy is *not* set to Auto Expand and the snap pool is running out of free space, you can manually expand the snap pool.

For expansion to succeed, the vdisk must have free space and sufficient resources. Because expansion does not require I/O to be stopped, the snap pool can continue to be used during expansion.

To expand a snap pool

1. In the Configuration View panel, right-click a volume and select **Tools > Expand Snap Pool**.
2. In the main panel, specify the amount of free space to add to the snap pool.
3. Click **Expand Snap Pool**. If the task succeeds, the snap pool's size is updated in the Configuration View panel.

Checking links to a remote system

After a remote system has been added, you can check the connectivity between host ports in the local system and the remote system. A host port in the local system can only link to other host ports with the same host interface, such as Fibre Channel (FC), in a remote system. When you check links, this panel will show this information for each linked host port in the local system:

- The link type
- The ID of the port in the local system
- The ID of each accessible port in the remote system

If a host port is not shown then either:

- It is not linked
- Its link type is not supported by both systems

To check links to a remote system

1. In the Configuration View panel, right-click a remote system and select **Tools > Check Remote System Link**.
2. Click **Check Links**.

Checking links in the local system

You can check the connectivity of host ports between controllers in the local system. A host port can only link to other ports with the same host interface, such as Fibre Channel (FC). When you check links, this panel will show this information for each linked host port in both controllers:

- The link type
- The port ID
- The ID of each linked port in the local system

To check links in the local system

1. In the Configuration View panel, right-click the local system and select **Tools > Check Local System Link**.
2. Click **Check Links**.

5 Viewing system status

Viewing information about the system

In the Configuration View panel, right-click the system and select **View > Overview**. The System Overview table shows:

- The system's health:
  - OK. The system is operating normally.
  - Degraded. At least one component is degraded.
  - Fault. At least one component has a fault.
  - N/A. Health is not available.
- The system's total storage space
- The health, quantity, and storage space of enclosures, disks, and vdisks
- The quantity and storage space of volumes and snap pools
- The quantity of snapshots and task schedules
- Configuration limits, licensed features, and versions of controller firmware and hardware

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

System properties

When you select the System component a table shows the system's health, name, contact, location, information (description), vendor name, product ID, product brand, SCSI vendor ID, SCSI vendor ID, and supported locales (languages).

A second table shows the system's redundancy mode and status, and each controller's status.

Enclosure properties

When you select the Enclosure component a table shows each enclosure's health, ID, WWN, vendor, model, and quantity of disk slots.

Disk properties

When you select the Disks component a table shows each disk's health, enclosure ID, slot number, serial number, vendor, model, firmware revision, type, usage, status, and size. How Used values are described in the disk properties section of Viewing information about a vdisk on page 90.

Vdisk properties

When you select the Vdisks component a table shows each vdisk's health, name, size, free space, RAID level, status, and disk type. Status values are described in the vdisk properties section of Viewing information about a vdisk on page 90.

Volume properties

When you select the Volumes component a table shows each volume's name, serial number, size, and vdisk name.

Snap-pool properties

When you select the Snap Pools component a table shows each snap pool's name, serial number, size, free space, master volumes, snapshots, and vdisk name.

Snapshot properties

When you select the Snapshots component a table shows each snapshot's name, serial number, source volume, snap-pool name, amounts of snap data, unique data, and shared data, and vdisk name.

- Snap data is the total amount of data associated with the specific snapshot (data copied from a source volume to a snapshot and data written directly to a snapshot).
- Unique data is the amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.
- Shared data is the amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.

Schedule properties

When you select the Schedules component a table shows each schedule's name, specification, status, next run time, task type, task status, and task state.

For the selected schedule, three tables appear. The first table shows schedule details and the second table shows task details. For a task of type TakeSnapshot, the third table shows the name and serial number of each snapshot that the task has taken and is retaining.

Configuration limits

When you select the Configuration Limits component a table shows the maximum quantities of vdisks, volumes, LUNs, disks, and host ports that the system supports.

Licensed features

When you select the Licensed Features component a table shows the status of licensed features.

Version properties

When you select the Versions component a table shows the versions of firmware and hardware in the system.

Viewing the system event log

In the Configuration View panel, right-click the system and select **View > Event Log**. The System Events panel shows the 100 most recent events that have been logged by either controller. All events are logged, regardless of event-notification settings. Click the buttons above the table to view all events, or only critical, warning, or informational events.

The event log table shows the following information:

- Severity.

  Critical. A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.

  Error. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.

  Warning. A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.

  Informational. A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.
- Time. Date and time when the event occurred, shown as *year-month-day hour:minutes:seconds* in Coordinated Universal Time (UTC). Time stamps have one-second granularity.
- Event ID. An identifier for the event. The prefix A or B identifies the controller that logged the event.

- Code. Event code that helps you and support personnel diagnose problems. For event-code descriptions and recommended actions, see the event descriptions reference guide.
- Message. Information about the event.

NOTE: If you are having a problem with the system or a vdisk, check the event log before calling technical support. Event messages might enable you to resolve the problem.

When reviewing events, do the following:

1. For any critical, error, or warning events, look for recommended actions in the event descriptions reference guide.

   Identify the primary events and any that might be the cause of the primary event. For example, an over-temperature event could cause a disk failure.
2. View the event log and locate other critical/error/warning events in the sequence for the controller that reported the event.

   Repeat this step for the other controller if necessary.
3. Review the events that occurred before and after the primary event.

   During this review you are looking for any events that might indicate the cause of the critical/error/warning event. You are also looking for events that resulted from the critical/error/warning event, known as secondary events.
4. Review the events following the primary and secondary events.

   You are looking for any actions that might have already been taken to resolve the problems reported by the events.

Viewing information about all vdisks

In the Configuration View panel, right-click **Vdisks** and select **View > Overview**. The Vdisks Overview table shows the overall health, quantity, capacity, and space usage of existing vdisks. For descriptions of storage-space color codes, see About storage-space color codes on page 31.

For each vdisk, the Vdisks table shows the following details:

- Health.

  OK. The vdisk is online with all disks working.

  Degraded. The vdisk is being reconstructed, as shown by its Current Job property; or, a RAID-6 vdisk has degraded performance due to one missing disk but remains fault tolerant. You can use a degraded RAID-6 vdisk but resolve the problem as soon as possible.

  Fault. The vdisk can perform I/O functions for hosts but is not fault tolerant. Review the status information and take the appropriate action, such as replacing a disk. You can use the vdisk but resolve the problem as soon as possible.

  N/A. Health is not available.
- Name. Vdisk name.
- Size. Total storage space in the vdisk.
- Free. Available space in the vdisk.
- RAID. RAID level of the vdisk and all of its volumes.
- Status.
  - CRIT: Critical. The vdisk is online but isn't fault tolerant because some of its disks are down.
  - FTDN: Fault tolerant with down disks. The vdisk is online and fault tolerant, but some of its disks are down.
  - FTOL: Fault tolerant and online.
  - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.

- QTCR: Quarantined critical. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed. For instance, one disk is missing from a mirror or RAID-5.
- QTDN: Quarantined with down disks. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed and would be fault tolerant. For instance, one disk is missing from a RAID-6.
- QTOF: Quarantined offline. The vdisk is offline and quarantined because multiple disks are missing and user data is incomplete.
- STOP: The vdisk is stopped.
- UNKN: Unknown.
- UP: Up. The vdisk is online and does not have fault-tolerant attributes.

- Disk Type. SAS (dual port), SAS-S (single port), SATA (dual port), or SATA-S (single port).
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Disks. Quantity of disks in the vdisk.
- Spares. Quantity of dedicated spares in the vdisk.

Viewing information about a vdisk

In the Configuration View panel, right-click a vdisk and select **View > Overview**. The Vdisks Overview table shows:

- The overall health, capacity, and space usage of the vdisk
- The overall health, quantity, capacity, and space usage of disks in the vdisk
- The quantity, capacity, and space usage of volumes in the vdisk
- The quantity, capacity, and space usage of snap pools in the vdisk

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

Vdisk properties

When you select the Vdisk component, the Properties for *Vdisk* table shows:

- Health.

  OK. The vdisk is online with all disks working.

  Degraded. The vdisk is being reconstructed, as shown by its Current Job property; or, a RAID-6 vdisk has degraded performance due to one missing disk but remains fault tolerant. You can use a degraded RAID-6 vdisk but resolve the problem as soon as possible.

  Fault. The vdisk can perform I/O functions for hosts but is not fault tolerant. Review the status information and take the appropriate action, such as replacing a disk. You can use the vdisk but resolve the problem as soon as possible.

  N/A. Health is not available.
- Health Reason. Shows more information about the vdisk's health.
- Name. Vdisk name.
- Size. Total storage space in the vdisk.
- Free. Available space in the vdisk.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Serial Number. Vdisk serial number.
- RAID. RAID level of the vdisk and all of its volumes.
- Disks. Quantity of disks in the vdisk.

- Spares. Quantity of dedicated spares in the vdisk.
- Chunk Size.
  - For RAID levels except NRAID, RAID 1, and RAID 50, the configured chunk size for the vdisk.
  - For NRAID and RAID 1, chunk size has no meaning and is therefore shown as not applicable (N/A).
  - For RAID 50, the vdisk chunk size calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). For a vdisk configured to use 32-KB chunk size and 4-disk sub-vdisks, the value would be `96k` (32KB x 3).
- Created. Date and time when the vdisk was created.
- Minimum Disk Size. Capacity of the smallest disk in the vdisk.
- Status.
  - CRIT: Critical. The vdisk is online but isn't fault tolerant because some of its disks are down.
  - FTDN: Fault tolerant with down disks. The vdisk is online and fault tolerant, but some of its disks are down.
  - FTOL: Fault tolerant and online.
  - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.
  - QTCR: Quarantined critical. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed. For instance, one disk is missing from a mirror or RAID-5.
  - QTDN: Quarantined with down disks. The vdisk is offline and quarantined because at least one disk is missing; however, the vdisk could be accessed and would be fault tolerant. For instance, one disk is missing from a RAID-6.
  - QTOF: Quarantined offline. The vdisk is offline and quarantined because multiple disks are missing and user data is incomplete.
  - and user data is incomplete.
  - STOP: The vdisk is stopped.
  - UNKN: Unknown.
  - UP: Up. The vdisk is online and does not have fault-tolerant attributes.
- Current Job. If a utility is running on the vdisk, this field shows the utility's name and progress.
- Drive Spin Down Vdisk Enable. Shows whether drive spin down is enabled or disabled for this vdisk.

Disk properties

When you select the Disks component, a Disk Sets table and enclosure view appear. The Disk Sets table shows:

- Total Space. Total storage space in the vdisk, followed by a color-coded measure of how the space is used.
- Type. For RAID 10 or RAID 50, the sub-vdisk that the disk is in; for other RAID levels, the disk's RAID level; or SPARE.
- Disk Type. SAS (dual port), SAS-S (single port), SATA (dual port), or SATA-S (single port).
- Disks. Quantity of disks in the vdisk or sub-vdisk.
- Size. Total capacity of the disks in the vdisk or sub-vdisk.

The enclosure view table has two tabs. The Tabular tab shows:

- Health. Shows whether the disk is healthy or has a problem.

  OK. The disk is operating normally.

  Fault. The disk has failed.

  Degraded. The disk's operation is degraded. If you find no related event in the event log, this may indicate a hardware problem.

  N/A. Health is not available.
- Name. System-defined disk name using the format Disk-*enclosure-number.disk-slot-number*.

- Type. SAS (dual port), SAS-S (single port), SATA (dual port), or SATA-S (single port).
- State. Shows how the disk is used:
  - If the disk is in a vdisk, its RAID level
  - AVAIL: Available
  - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
  - SPARE: Spare assigned to a vdisk
  - GLOBAL SP: Global spare
  - LEFTOVR: Leftover

  Also shows any job running on the disk:
  - DRSC: The disk is being scrubbed
  - EXPD: The vdisk is being expanded
  - INIT: The vdisk is being initialized
  - RCON: The vdisk is being reconstructed
  - VRFY: The vdisk is being verified
  - VRSC: The vdisk is being scrubbed
- Size. Disk capacity.
- Enclosure. Name of the enclosure containing the disk.
- Serial Number. Disk serial number.
- Status. Up (operational) or Not Present.

The Graphical tab shows the locations of the vdisk's disks in system enclosures and each disk's Health and State.

Volume properties

When you select the Volumes component, the Volumes table shows:

- The volume's name, serial number, and size
- The name of the vdisk containing the volume

Snap-pool properties

When you select the Snap Pools component, the Snap Pools table shows:

- The snap pool's name, serial number, size, and free space
- The quantity of master volumes and snapshots associated with the snap pool
- The name of the vdisk containing the snap pool

Viewing information about a volume

In the Configuration View panel, right-click a volume and select **View > Overview**. The Volume Overview table shows:

- The capacity and space usage of the volume
- The quantity of mappings for the volume
- The quantity of task schedules for the volume
- As described in Viewing replication properties, addresses, and images for a volume on page 119: the quantities of replication addresses and replication images for the volume

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

Volume properties

When you select the Volume component, the Properties for *Volume* table shows:

- Vdisk Name. Name of the vdisk that the volume is in.
- Name. Volume name.
- Size. Volume size.
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Serial Number. Volume serial number.
- Cache Write Policy. Write-back or write-through. See Using write-back or write-through caching on page 22.
- Cache Optimization. Standard or super-sequential. See Optimizing read-ahead caching on page 23.
- Read Ahead Size. See Optimizing read-ahead caching on page 23.
- Type. Standard volume, master volume, or snapshot.
- Progress. If the volume is being created by a volume-copy operation, the percent complete.

Mapping properties

When you select the Maps component, the Maps for *Volume* table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Name. Host name.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

Schedule properties

If any schedules exist for this volume, when you select the Schedules component, the Schedules table shows each schedule's name, specification, status, next run time, task type, task status, and task state. For the selected schedule, two tables appear.

The Schedule Details table shows:

- Schedule Name. Schedule name.
- Schedule Specification. The schedule's start time and recurrence or constraint settings.
- Status.
  - Uninitialized: Schedule is not yet ready to run.
  - Ready: Schedule is ready to run.
  - Suspended: Schedule is suspended.
  - Expired: Schedule has expired.
  - Invalid: Schedule is invalid.
- Next Time.

The Task Details table shows different properties depending on the task type. Properties shown for all task types are:

- Task Name. Task name.
- Task Type. ReplicateVolume, ResetSnapshot, TakeSnapshot, or VolumeCopy.
- Status.
  - Uninitialized: Task is not yet ready to run.
  - Ready: Task is ready to run.
  - Active: Task is running.

    - Error: Task has an error.
    - Invalid: Task is invalid.
- Task State. Current step of task processing. Steps vary by task type.
- Source Volume. Name of the volume to snap, copy, or replicate.
- Source Volume Serial. Source volume serial number.
- Destination Vdisk. Name of the destination vdisk for a volume copy.
- Destination Vdisk Serial. Destination vdisk serial number.
- Prefix. Label that identifies snapshots, volume copies, or replication images created by this task.
- Count. Number of snapshots to retain with this prefix. When a new snapshot exceeds this limit, the oldest snapshot with the same prefix is deleted.
- Last Created. Name of the last snapshot, volume copy, or replication image created by the task.
- Last Used Snapshot. For a task whose replication mode is last-snapshot, the name of the last snapshot used for replication.
- Snapshot Name. Name of the snapshot to reset.
- Snapshot Serial. Snapshot serial number.
- Mode. Replication mode:
    - new-snapshot: Replicate a new snapshot of the primary volume.
    - last-snapshot: Replicate the most recent existing snapshot of the primary volume.

For a TakeSnapshot task, the Retained Set table shows the name and serial number of each snapshot that the task has taken and is retaining.

Viewing information about a snapshot

In the Configuration View panel, right-click a snapshot and select **View > Overview**. The Snapshot Overview table shows:

- The capacity and space usage of the snapshot
- The quantity of mappings for the snapshot
- The quantity of task schedules for the snapshot

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

Snapshot properties

When you select the Snapshot component, the Properties for Snapshot table shows:

- Vdisk Name.
- Serial Number. Snapshot serial number.
- Name. Snapshot name.
- Creation Date/Time.
- Status.
- Status-Reason.
- Source Volume. Name of the volume that the snapshot was taken of.
- Snap-pool Name.
- Snap Data. The total amount of data associated with the specific snapshot (data copied from a source volume to a snapshot and data written directly to a snapshot).
- UniqueData. The amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.
- SharedData. The amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that

is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.

- Priority. Retention priority for the snapshot, based on the snapshot attributes and the user-defined priority for the snapshot type.
- User Priority. User-defined priority for the snapshot type.
- Type.
  - Standard snapshot: Snapshot of a master volume that consumes a snapshot license.
  - Replication snapshot: For a primary or secondary volume, a snapshot that was created by a replication operation but is not a sync point.
  - Replication snapshot (Replicating): For a primary volume, a snapshot that is being replicated to a secondary system.
  - Replication snapshot (Current sync point): For a primary or secondary volume, the latest snapshot that is copy-complete on any secondary system in the replication set.
  - Replication snapshot (Common sync point): For a primary or secondary volume, the latest snapshot that is copy-complete on all secondary systems in the replication set.
  - Replication snapshot (Old Common sync point): For a primary or secondary volume, a common sync point that has been superseded by a new common sync point.
  - Replication snapshot (Only sync point): For a primary or secondary volume, the only snapshot that is copy-complete on any secondary system in the replication set.
  - Replication snapshot (Queued): For a primary volume, a snapshot associated with a replication operation that is waiting for a previous replication operation to complete.
  - Replication snapshot (Awaiting replicate): For a primary volume, a snapshot that is waiting to be replicated to a secondary system.

Mapping properties

When you select the Maps component, the Maps for *Volume* table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Name. Host name.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

Schedule properties

If any schedules exist for the snapshot, when you select the Schedules component, the Schedules table shows information about each schedule. For the selected schedule, the Schedule Details table shows:

- Schedule Name.
- Schedule Specification.
- Schedule Status.
- Next Time.
- Task Type.
- Task Status.
- Task State.
- Source Volume.
- Source Volume Serial.
- Prefix.
- Count.
- Last Created.

Viewing information about a snap pool

In the Configuration View panel, right-click a snap pool and select **View > Overview**. The Snap Pool Overview table shows:

- The capacity and space usage of the snap pool
- The quantity of volumes using the snap pool
- The quantity of snapshots in the snap pool

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

Snap-pool properties

When you select the Snap Pool component, two tables appear. The first table shows the snap pool's name, serial number, size (total capacity), vdisk name, and free space, the number of snapshots in the snap pool, and its status. The status values are:

- Available: The snap pool is available for use.
- Offline: The snap pool is not available for use, as in the case where its disks are not present.
- Corrupt: The snap pool's data integrity has been compromised; the snap pool can no longer be used.

The second table shows the snap pool's threshold values and associated policies. Three thresholds are defined:

- Warning: The snap pool is moderately full. When this threshold is reached, an event is generated to alert the administrator. The default value is 75%.
- Error: The snap pool is nearly full and unless corrective action is taken, snapshot data loss is probable. When this threshold is reached, an event is generated to alert the administrator and the associated snap-pool policy is triggered. The default is 90%.
- Critical: The snap pool is 98% full and data loss is imminent. When this threshold is reached, an event is generated to alert the administrator and the associated snap-pool policy is triggered.

The following policies are defined:

- Auto Expand: Automatically expand the snap pool by the indicated expansion-size value. This is the default policy for the Error threshold.

  If the snap pool's space usage reaches the percentage specified by its error threshold, the system will log Warning event 230 and will try to automatically expand the snap pool by the snap pool's expansion-size value. If the snap pool cannot be expanded because there is not enough available space in its vdisk, the system will log Warning event 444 and will automatically delete the oldest snapshot that is not a current sync point.
- Delete Oldest Snapshot: Delete the oldest snapshot.
- Delete Snapshots: Delete all snapshots. This is the default policy for the Critical threshold.
- Halt Writes: Halt writes to all master volumes and snapshots associated with the snap pool.
- Notify Only: Generates an event to notify the administrator. This is the only policy for the Warning threshold.
- No Change: Take no action.

NOTE: The policies Delete Oldest Snapshot and Delete Snapshots do not apply business logic to the delete decision and may delete snapshots that are mounted/presented/mapped or modified. You may set retention priorities for a snap pool as a way of suggesting that some snapshots are more important than others, but these priorities do not ensure any specific snapshot is protected.

For details about setting snap-pool thresholds and policies, see the CLI reference guide.

Volume properties

When you select the Client Volumes component, a table shows each volume's name, serial number, size, vdisk name, and vdisk serial number.

Snapshot properties

When you select the Resident Snapshots component, a table shows each volume's name, serial number, and amounts of snap data, unique data, and shared data.

Snap data is the total amount of data associated with the specific snapshot (data copied from a source volume to a snapshot and data written directly to a snapshot).

Unique data is the amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.

Shared data is the amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.

Viewing information about all hosts

In the Configuration View panel, right-click **Hosts** and select **View > Overview**. The Hosts table shows the quantity of hosts configured in the system.

For each host, the Hosts Overview table shows the following details:

- Host ID. WWPN or IQN.
- Name. User-defined nickname for the host.
- Discovered. If the host was discovered and its entry was automatically created, Yes. If the host entry was manually created, No.
- Mapped. If volumes are mapped to the host, Yes; otherwise, No.
- Host Type. FC or iSCSI.

Viewing information about a host

In the Configuration View panel, right-click a host and select **View > Overview**. The Host Overview table shows:

- Host properties
- The quantity of mappings for the host

Select a component to see more information about it.

Host properties

When you select the Host component, the Properties for *Host* table shows:

- Host ID. WWPN or IQN.
- Name. User-defined nickname for the host.
- Discovered. If the host was discovered and its entry was automatically created, Yes. If the host entry was manually created, No.
- Mapped. If volumes are mapped to the host, Yes; otherwise, No.
- Host Type. FC or iSCSI.

Mapping properties

When you select the Maps component, the Maps for *Host* table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Name. Volume name.
- Serial Number. Volume serial number.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

Viewing information about an enclosure

In the Configuration View panel, right-click an enclosure and select **View > Overview**. You can view information about the enclosure and its components in a front or rear graphical view, or in a front or rear tabular view.

- Front Graphical. Shows a graphical view of the front of each enclosure and its disks.
- Front Tabular. Shows a tabular view of each enclosure and its disks.
- Rear Graphical. Shows a graphical view of components at the rear of the enclosure.
- Rear Tabular. Shows a tabular view of components at the rear of the enclosure.

In any of these views, select a component to see more information about it. Components vary by enclosure model. If any components are unhealthy, a table at the bottom of the panel identifies them.

Enclosure properties

When you select an enclosure, a table shows:

- Health.
  - OK. The enclosure is operating normally.
  - Degraded. At least one component is degraded.
  - Fault. At least one component has a fault.
  - N/A. Health is not available.
- Health Reason.
- Enclosure ID.
- Vendor.
- Model.
- Disk Slots.
- Enclosure WWN.
- Mid-plane Serial Number.
- Part Number.
- Manufacturing Date.
- Manufacturing Location.
- Revision.
- EMP A Revision. Firmware revision of the Enclosure Management Processor in controller module A's Expander Controller.
- EMP B Revision. Firmware revision of the Enclosure Management Processor in controller module B's Expander Controller.
- EMP A Bus ID.
- EMP B Bus ID.
- EMP A Target ID.
- EMP B Target ID.

- Enclosure Power (watts).
- PCIe 2-Capable. Shows whether the enclosure is capable of using PCI Express version 2.

Disk properties

When you select a disk, a table shows:

- Health.

  OK. The disk is operating normally.

  Degraded. The disk's operation is degraded. If you find no related event in the event log, this may indicate a hardware problem.

  Fault. The disk has failed.

  N/A. Health is not available.
- Health Reason.
- Enclosure ID.
- Slot.
- How Used.
  - AVAIL: Available.
  - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
  - GLOBAL SP: Global spare.
  - LEFTOVR: Leftover.
  - VDISK: Used in a vdisk.
  - VDISK SP: Spare assigned to a vdisk.
- Status.
  - Up: The disk is present and is properly communicating with the expander.
  - Spun Down: The disk is present and has been spun down by the DSD feature.
  - Warning: The disk is present but the system is having communication problems with the disk LED processor. For disk and midplane types where this processor also controls power to the disk, power-on failure will result in Error status.
  - Error: The disk is present but is not detected by the expander.
  - Unknown: Initial status when the disk is first detected or powered on.
  - Not Present: The disk slot indicates that no disk is present.
- Type.
  - SAS: Dual-port SAS.
  - SAS-S: Single-port SAS.
  - SATA: Dual-port SATA.
  - SATA-S: Single-port SATA.
  - sSAS: Dual-port SAS SSD.
  - sSATA: Dual-port SATA SSD.
- Vendor.
- Model.
- Size.
- RPM (x1000).
- Transfer Rate. The data transfer rate in Gbit per second.

  Some 6-Gbps disks might not consistently support a 6-Gbps transfer rate. If this happens, the controller automatically adjusts transfers to those disks to 3 Gbps, increasing reliability and reducing error messages with little impact on system performance. This rate adjustment persists until the controller is restarted or power-cycled.
- Revision. Disk firmware revision number.
- Serial Number.

- Current Job.
  - DRSC: Disks in the vdisk are being scrubbed.
  - EXPD: The vdisk is being expanded.
  - INIT: The vdisk is being initialized.
  - RCON: The vdisk is being reconstructed.
  - VRFY: The vdisk is being verified.
  - VRSC: The vdisk is being scrubbed.
- SMART. Shows whether Self-Monitoring Analysis and Reporting Technology is enabled. For more information, see Configuring SMART on page 45.
- Current Owner. For the disk's vdisk, either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Drive Spin Down Count. How many times the disk has been spun down.

Power supply properties

When you select a power supply, a table shows:

- Health.
  - OK. The power supply is operating normally.
  - Degraded. The power supply's operation is degraded.
  - Fault. The power supply has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Model.
- Vendor.
- Location.
- Serial Number.
- Revision.
- Part Number.
- Manufacturing Date.
- Manufacturing Location.

Controller module properties

When you select a controller module, a table shows:

- Health.
  - OK. The controller module is operating normally.
  - Degraded. The controller module's operation is degraded.
  - Fault. The controller module has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Controller ID.
- Description.
- CPLD Version.
- Storage Controller Code Version.
- Model.
- Storage Controller CPU Type.
- Serial Number.

- Part Number.
- Position.
- Hardware Version.
- Revision.
- Manufacturing Date.
- Manufacturing Location.

Controller module: network port properties

When you select a network port, a table shows:

- Health.
  - OK. The port is operating normally.
  - Degraded. The port's operation is degraded.
  - Fault. The port has failed.
  - N/A. Health is not available.
- Health Reason.
- MAC Address.
- Addressing Mode.
- IP Address.
- Gateway.
- Subnet Mask.

Controller module: host port properties

When you select a host port, a table shows:

- Health.
  - OK. The port is operating normally.
  - Degraded. The port's operation is degraded.
  - Fault. The port has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Port ID.
- Media Type.
- Target ID.
- Configured Speed.
- Actual Speed.

Controller module: expansion port properties

When you select an expansion (Out) port, a table shows:

- Health.
  - OK. The port is operating normally.
  - Degraded. The port's operation is degraded.
  - Fault. The port has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Name.

Controller module: CompactFlash properties

When you select a CompactFlash card, a table shows:

- Health.
  - OK. The card is operating normally.
  - Fault. The card has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Cache Flush.

Drive enclosure: I/O module properties

When you select an I/O module, a table shows:

- Health.
  - OK. The I/O module is operating normally.
  - Degraded. The I/O module's operation is degraded.
  - Fault. The I/O module has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Controller ID.

I/O module: In port properties

When you select an In port, a table shows:

- Health.
  - OK. The port is operating normally.
  - Degraded. The port's operation is degraded.
  - Fault. The port has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Name.

I/O module: Out port properties

When you select an Out port, a table shows:

- Health.
  - OK. The port is operating normally.
  - Degraded. The port's operation is degraded.
  - Fault. The port has failed.
  - N/A. Health is not available.
- Health Reason.
- Status.
- Name.

Viewing information about a remote system

In the Configuration View panel, right-click a remote system and select **View > Overview**. The System Information table shows:

- The username and network-port IP addresses that are configured on the local system to access the remote system. The configured password is not shown.
- Information such as the system name, location, and status that is read from the remote system.

To sign in to the remote system, click one of its IP address links.

6 Using AssuredRemote to replicate volumes

About the AssuredRemote replication feature

AssuredRemote™ replication is a licensed feature for disaster recovery. This feature performs asynchronous (batch) replication of block-level data from a volume on a local storage system to a volume that can be on the same system or on a second, independent system. This second system can be located at the same site as the first system or at a different site.

TIP: For guidelines about setting up and using the AssuredSnap, AssuredCopy, and AssuredRemote features singly or together, see the document *AssuredSAN 3000 Series Using Data Protection Software*.

A typical replication configuration involves these physical and logical components:

- A host connected to a local storage system, which is networked via FC or iSCSI ports to a remote storage system as described in installation documentation.
- *Remote system* definition. A management object on the local system that enables the MCs in the local system and in the remote system to communicate and exchange data.
- *Replication set*. Associated master volumes that are enabled for replication and that typically reside in two physically or geographically separate storage systems. These volumes are also called replication volumes.
- *Primary volume*. The volume that is the source of data in a replication set and that can be mapped to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The primary volume exists in a primary vdisk in the primary system.
- *Secondary volume*. The volume that is the destination for data in a replication set and that is not accessible to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The secondary volume exists in a secondary vdisk in a secondary system.
- *Replication snapshot*. A special type of snapshot that preserves the state of data of a replication set's primary volume as it existed when the snapshot was created. For a primary volume, the replication process creates a replication snapshot on both the primary system and, when the replication of primary-volume data to the secondary volume is complete, on the secondary system. Replication snapshots are unmappable and are not counted toward a license limit, although they are counted toward the system's maximum number of volumes. A replication snapshot can be exported to a regular, licensed snapshot.
- *Replication image*. A conceptual term for replication snapshots that have the same image ID in primary and secondary systems. These synchronized snapshots contain identical data and can be used for disaster recovery.

Replication process overview

As a simplified overview of the remote-replication process, it can be configured to provide a single point-in-time replication of volume data or a periodic delta-update replication of volume data.

The periodic-update process has multiple steps. At each step, matching snapshots are created: in the primary system, a replication snapshot is created of the primary volume's current data; this snapshot is then used to copy new (delta) data from the primary volume to the secondary volume; then in the secondary system, a matching snapshot is created for the updated secondary volume. This pair of matching snapshots establishes a replication sync point and these sync points are used to continue the replication process. Following next is a step-by-step example of the remote-replication process.

The following figure illustrates three replication sets in use by two hosts:

- The host in New York is mapped to and updates the Finance volume. This volume is replicated to the host in Munich.

- The host in Munich is mapped to and updates the Sales and Engineering volumes. The Sales volume is replicated from System 2 to System 3 in the Munich DATA center. The Engineering volume is replicated from System 3 in Munich to System 1 in New York.

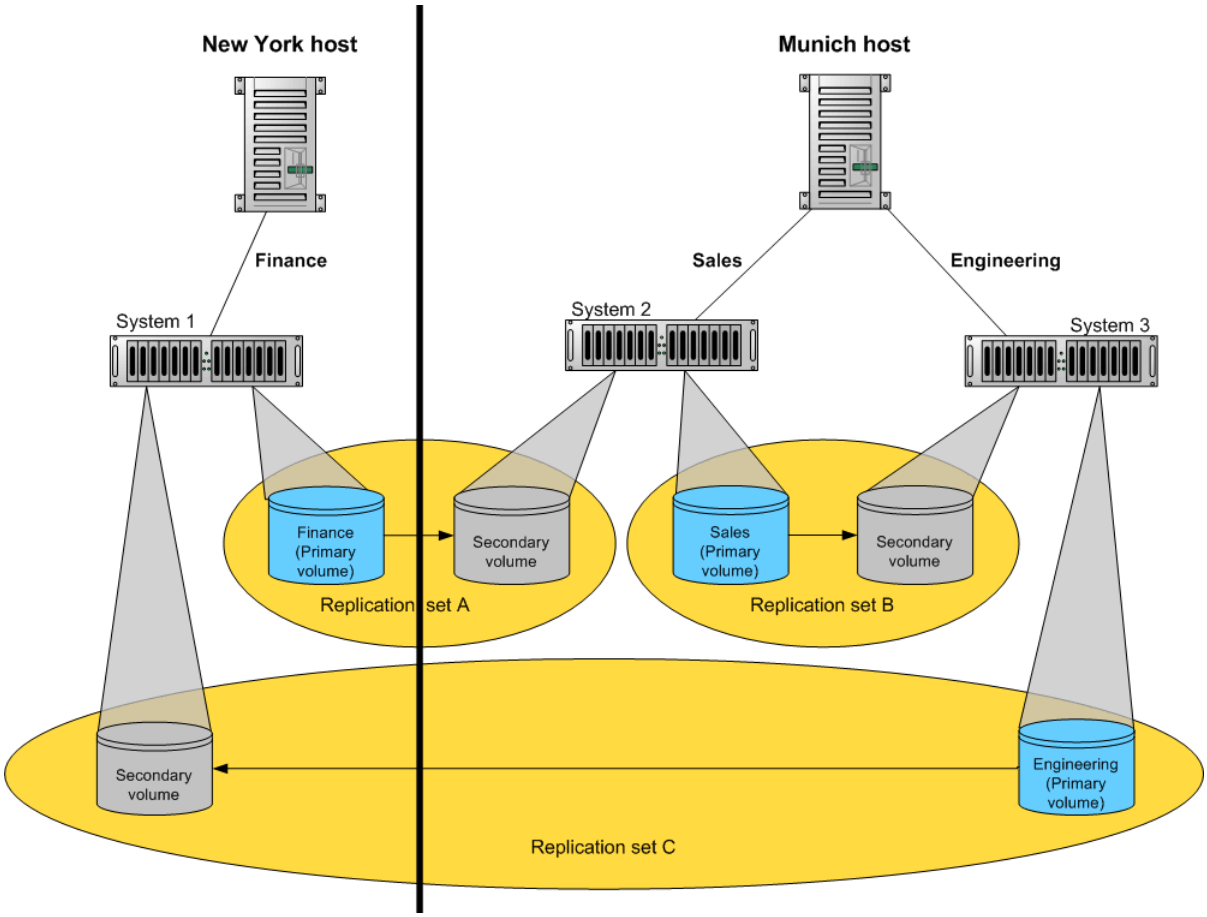


Figure 4 Intersite and intrasite replication sets

Remote replication uses snapshot functionality to track the data to be replicated and to determine the differences in data updated on the master volume, minimizing the amount of data to be transferred. Snapshots created by the remote replication process are a special form called *replication snapshots*, which do not count against snapshot license limits.

In order to perform a replication, a snapshot of the primary volume is taken, creating a point-in-time image of the data. This point-in-time image is then replicated to the secondary volume by copying the data represented by the snapshot using a transport medium such as TCP/IP (iSCSI) or Fibre Channel. The first replication copies all data from the primary volume to the secondary volume; subsequent replications use sparse snapshots.

Replication snapshots are retained for both the primary volume and the secondary volume. When a matching pair of snapshots is retained for both volumes, the matching snapshots are referred to as *replication sync points*. The two snapshots (one on each volume) are used together as a synchronization reference point, minimizing the amount of data to transfer. The two snapshots in a sync point are assigned the same *image ID*, which uniquely identifies that the data in those snapshots are from the same point-in-time image and are block-for-block identical.

When a replication snapshot is created from a standard snapshot, while that snapshot remains present the replication snapshot's total data represented is zero bytes. This behavior occurs because the snapshot data remains associated with the standard snapshot and there is no data specifically associated with the replication snapshot. If the standard snapshot is deleted, its data becomes associated with (is preserved by) the replication snapshot and the replication snapshot's size changes to reflect the size of the deleted snapshot.

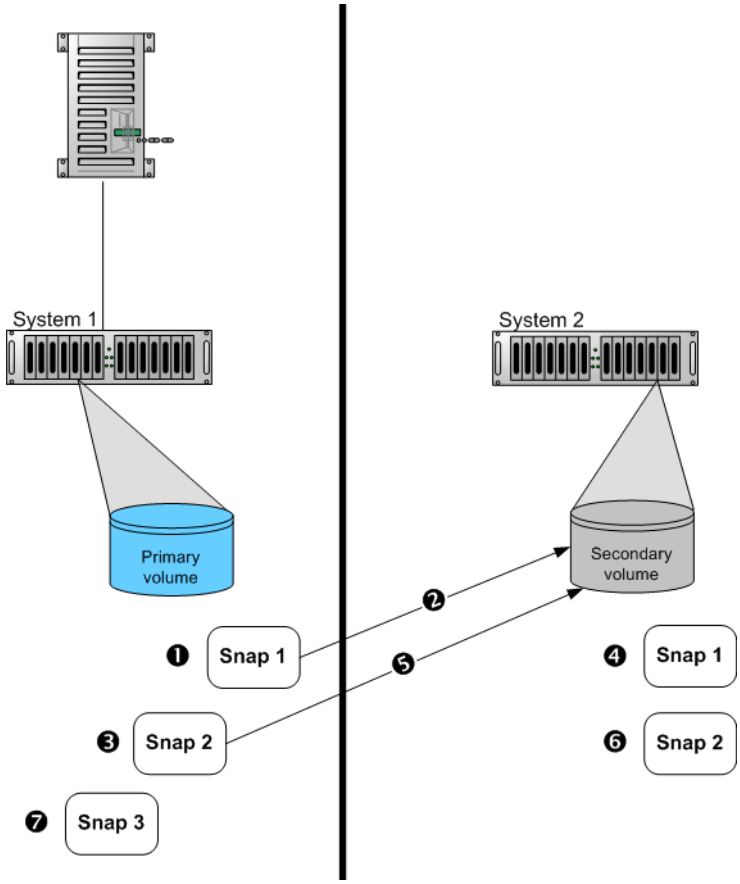
An added benefit of using snapshots for replication is that these snapshots can be kept and restored later in the event of a non-hardware failure, such as virus attack. Since the replication source is a snapshot, any writes performed on the primary volume after the snapshot is taken are not replicated by that task. This gives you more control over what is contained in each replication image.

NOTE: Because replication is not synchronous (continuous), data in a secondary volume is only as current as the last replication that completed successfully. Replications can be performed manually or scheduled.

Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

Replication actions

The following figure illustrates actions that occur during a series of replications from System 1 to System 2.



1. Take initial snapshot and initiate replication.
2. Initial replication consists of a full data copy.
3. Take second snapshot and request replication. This can be taken while the initial replication is in progress.
4. Snapshot taken on secondary volume. This is the first replication sync point.
5. When the initial replication is complete, the second replication automatically starts. Only the data changed since Snap 1 is replicated.
6. Second snapshot taken on secondary volume. This is the second sync point.
7. Other snapshots can be taken and replication initiated on the primary volume while replication is in progress. These snapshots are queued waiting for prior replications to complete. These replication snapshots will not become sync points until their replications are complete.

Figure 5 Actions that occur during a series of replications

The figure above illustrates initial, delta, and queued replications:

- Initial replication: When the first replication is initiated, a snapshot of the primary volume is taken and every block of data is then copied to the secondary volume. When the copy is complete, the first snapshot is taken on the secondary volume, creating the first sync point. This sync point can be used to determine the delta data from that sync point to a later snapshot. Actions 1–4 are the initial replication.
- Delta replications: Delta data is the "list" of 64-KB blocks that differs between the last snapshot replicated and the next snapshot to be replicated. This delta data is then replicated from the replication snapshot on the primary volume to the secondary volume. Once the initial replication has completed, all future replications for that replication set will be delta replications so long as sync points are maintained. Action 5 is a delta replication.
- Queued replications: New replications can be initiated while other replication snapshots are in the process of being replicated. This enables you to take snapshots at specific intervals while other replications are ongoing. Note that a replication that is initiated while another to the same secondary volume is ongoing will be queued, and will not begin to transfer data until the prior one completes. In action 3, Snap 2 is queued while Snap 1 is being replicated; in action 7, Snap 3 is queued while Snap 2 is being replicated.

An in-progress replication can be suspended, either manually by a user or automatically if a network error occurs. If you want the replication to continue, you must manually resume it; or, if you want to cancel the replication, you can abort it.

IMPORTANT: For a replication to begin, the controller that owns the secondary volume must have a link to the controller that owns the primary volume. This link must be of the type specified by the link-type parameter supplied during replication set creation or modification. If all links to the controller that owns the primary volume fail, but links remain between its partner controller and the controller that owns the secondary volume, replications currently in progress or queued may continue, but their progress may not be reported correctly; replications requested after the links fail will not start replicating. If the controller that owns the secondary volume loses all links to both controllers of the primary system, then the replications will suspend and progress will be updated appropriately; links from the partner controller of the controller that owns the secondary volumes are not considered for use. Replications that enter the suspended state must be resumed manually.

Performing initial replication locally or remotely

When you set up replication for a volume, you specify to use a secondary volume in a vdisk in either the local (primary) system or a remote (secondary) system.

- If the speed of the initial replication is most important, specify a vdisk that is owned by the same controller as the primary volume's vdisk in the local system.

  After replication is set up, you can perform the initial replication and then physically move the vdisk containing the secondary volume and its snap pool into a remote system. Moving a vdisk involves using RAIDar to detach the secondary volume and stop its vdisk, removing the vdisk's disks or enclosure, transporting the disks or enclosure to the remote location, inserting the disks or enclosure into the remote system, and using RAIDar to restart the vdisk and reattach the secondary volume. If the secondary volume's snap pool is in a different vdisk then that vdisk must also be stopped, moved, and restarted.
- If ease of setup is most important, specify a vdisk owned by either controller in a remote system. After replication is set up, you can start replication.

In either case, you must specify whether FC or iSCSI links will be used for replication between the primary and secondary systems and you cannot change this setting for the life of the replication set.

Remote replication disaster recovery

Replication can continue in the event of system faults such as:

- Temporary communication failure. Remote replication will retry replication operations according to user-configured policies.
- Controller failure. In a dual-controller system, failover will occur and the surviving controller will take over replication processing until controller recovery occurs.
- Disk or power supply failure.

If a disaster causes the primary volume to become inaccessible, you can set the secondary volume to the primary volume so that volume can be mapped to hosts. Disaster recovery requires user intervention because decisions must be made based on the data content of replication volumes and their snapshots.

1. Synchronize the secondary volume to a replication snapshot, preferably a replication sync point. Any data written to the primary volume since the last-completed replication will not be available.
2. After synchronization, set the secondary volume to be the new primary volume.
3. Map the new primary volume to hosts, as was the original primary volume.

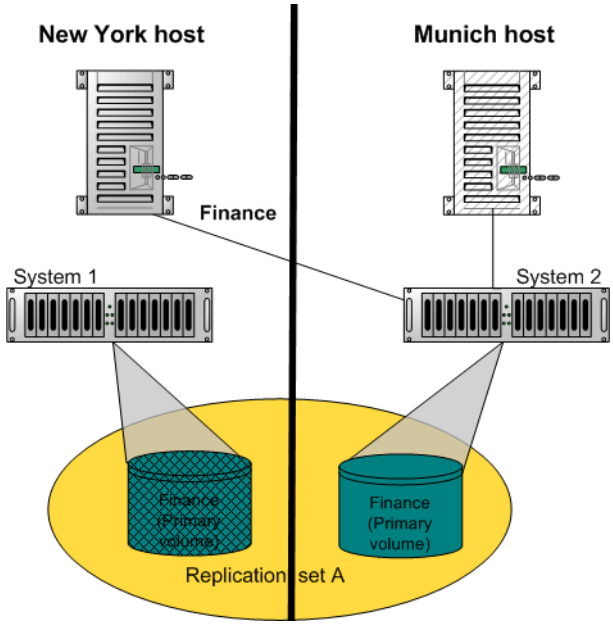


Figure 6 Example of primary-volume failure

If the original primary volume becomes accessible, you can set it to be the primary volume again.

1. Take a snapshot of the original primary volume. This preserves the volume's current data state for later comparison with the new primary volume.
2. Set the original primary volume to be a secondary volume.
3. Replicate any data written to the new primary volume to the original primary volume (now a secondary volume). This can be done as one or more replications. On the final replication, halt host access to the primary volume to ensure that all data has been transferred to the secondary volume.
4. Set the secondary volume (the original primary volume) to be the new primary volume.
5. You can now mount/present/map the snapshot taken in step 1 and compare it with the new primary volume to identify any data discrepancies and try to recover any data from the snapshot that would otherwise be lost. For example, you could use host file-system tools to find any files modified since a certain time, or for a database you could export any differing records from the snapshot and re-enter them into the current database.

Remote replication licensing

The Remote Replication and Snapshot features are separately licensed. Remote replication can operate without Snapshot being enabled; however, to get the most out of remote replication, it is recommended to enable both features. Normally, replication snapshots are not accessible to hosts. However, if Snapshot is enabled, a replication snapshot can be exported for use as a standard snapshot.

Related topics

- Installing a license on page 37
- Adding (page 50) or deleting (page 50) a remote system
- Checking links to a remote system on page 85
- Using the Replication Setup Wizard on page 110
- Replicating a volume (page 112) or a snapshot (page 114)
- Detaching (page 115) and reattaching (page 117) a secondary volume
- Stopping (page 116) and restarting (page 117) a vdisk
- Suspending (page 115), resuming (page 115), or aborting (page 115) a replication
- Exporting a replication image to a snapshot on page 118
- Changing the primary volume for a replication set on page 118
- Viewing replication properties, addresses, and images for a volume on page 119
- Viewing information about a replication image on page 121

Using the Replication Setup Wizard

If the system is licensed to use remote replication, you can use the Replication Setup Wizard to prepare to replicate an existing volume to another vdisk in the local system or to a remote system. Before using this wizard, read documentation and Resource Library guidelines for your product to learn about replication. Then plan the storage systems, replication mode, and volumes you want to use for the replication.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Select the primary volume, which is an existing volume or snapshot to replicate.
- Specify whether the replication mode will be local or remote. If the replication will be to a remote system that has not already been added to the local system, you can add it. To do so, you must know the user name and password of a Manage user on that system and the system's IP address.
- Specify the secondary volume. You can select an existing replication-prepared volume or specify to create a volume in an existing vdisk that has sufficient available space for the replicated data.
- Confirm changes and apply them.

IMPORTANT: Before starting this procedure, if you intend to use CHAP to authenticate iSCSI login requests between the local system and a remote system, do the following:

- Create a one-way CHAP record on each system. On the local system, the CHAP record must refer to the node name of the remote system. On the remote system, the CHAP record must refer to the node name of the local system. Both records must use the same secret. (Mutual CHAP is not used between storage systems. CHAP records' mutual fields can be set but are not used.) To create a CHAP record, see Configuring CHAP on page 72.
- After the CHAP records are created, enable CHAP on the primary system, the secondary system, or both. To enable CHAP, see Changing host interface settings on page 42.

If both records don't exist or don't use the same secret, replication-set creation will fail.

Step 1: Starting the wizard

1. In the Configuration View panel, right-click the system and select **Wizards > Replication Setup Wizard**. The wizard panel appears.
2. Click **Next** to continue.

Step 2: Selecting the primary volume

Select the volume whose data you want to replicate. If the volume has at least one snapshot, you can select a snapshot to be the replication source.

To select the primary volume

1. Set the options:
   - Select the vdisk that contains the volume to replicate. Only vdisks that contain at least one volume are listed for selection.
   - Select the volume to replicate. Only volumes that are not already part of a replication set are listed for selection.
2. Click **Next** to continue.

Step 3: Selecting the replication mode

Select the replication mode, which specifies whether the secondary volume is in the local system or a remote system. If you want to replicate to a remote system that hasn't already been added to the local system, you can add it.

To replicate within the local system

1. Select **Local Replication**.
2. Although it is recommended to check host-port links between controllers in the local system, if you already know the status of links you can clear the **Check Links** checkbox to skip this task.
3. Click **Next** to continue. If there are no links between the controllers, a message appears, and only vdisks and volumes that are owned by the same controller as the primary volume will appear in the next step.

To replicate to a remote system

1. Select **Remote Replication**.
2. In the Remote System list, look for the remote system that you want to use.
   - If you find the system, select it and continue with step 5.
   - If you don't find it, add it as described in step 3.
3. To add a remote system, in the Add new Remote System area:
   a. Enter the IP address of a network port on the remote system.
   b. Enter the user name of a user with a Manage role on the remote system.
   c. Enter that user's password.
   d. Click **Add Remote System**. If task succeeds, the new remote system appears in the Remote System list and is selected.
4. Although it is recommended to check host-port links between the two systems, this can take up to 3 minutes, so if you already know the status of links you can clear the **Check Links** checkbox to skip this task.
5. Click **Next** to continue. If there are no links to the remote system, a message appears and you cannot proceed. For a hybrid system, if only one link type is up, only that link type will appear in the next step.

Step 4: Selecting the secondary volume

Specify the secondary volume. You can select an existing replication-prepared volume or specify to create a volume in an existing vdisk that has sufficient available space for the replicated data. If no existing volumes are appropriate to use, the Secondary Volume options will be grayed out but you can still select a vdisk.

To specify the secondary volume

1. Either:
   - Select **Create new volume on vdisk** and select the vdisk where you want the secondary volume to be created.
   - Select **Use existing replication-prepared volume** and select an existing replication-prepared volume to be the secondary volume. Only replication-prepared volumes are listed for selection.
2. Select the link type used between the two systems.
3. Click **Next** to continue.

Step 5: Confirming replication settings

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

Replicating a volume

If the system is licensed to use remote replication, you can create a replication set that uses the selected volume as the primary volume, and to immediately start or schedule replication. The primary volume can be a standard volume or a master volume.

To create a replication set you must select a secondary system and a secondary vdisk or volume. The secondary system can be the local system, or a remote system added by using the Add Remote System panel.

You can select the local system if you intend to create the replication set on the local system and then physically move the secondary vdisk's disks (or enclosure) to a remote system. Otherwise, select a remote system that you've added to the local system.

IMPORTANT: A best practice is to schedule no more than three volumes to start replicating at the same time, and for those replications to recur no less than 60 minutes apart. If you schedule more replications to start at the same time, or schedule replications to start more frequently, some scheduled replications may not have time to complete.Before starting this procedure, if you intend to use CHAP to authenticate iSCSI login requests between the local system and a remote system, do the following:

- Create a one-way CHAP record on each system. On the local system, the CHAP record must refer to the node name of the remote system. On the remote system, the CHAP record must refer to the node name of the local system. Both records must use the same secret. (Mutual CHAP is not used between storage systems. CHAP records' mutual fields can be set but are not used.) To create a CHAP record, see Configuring CHAP on page 72.
- After the CHAP records are created, enable CHAP on the primary system, the secondary system, or both. To enable CHAP, see Changing host interface settings on page 42.

If both records don't exist or don't use the same secret, replication-set creation will fail.

NOTE: If replication requests are sent to a secondary system whose temporary replication license has expired, the requests are queued but are not processed, and the secondary system reports event 472. If this condition occurs, check for this event in the event log, event-notification emails, and SNMP traps. To continue using replication, purchase a permanent replication license.

To create a replication set and optionally start or schedule replication

1. In the Configuration View panel, right-click a volume and select **Provisioning > Replicate Volume**.
2. In the main panel, set the destination options:
   - Secondary System. Select a storage system to replicate the volume to.
   - Secondary Volume. Select an existing vdisk or an existing replication-prepared volume to be the secondary volume. Vdisks listed for selection have enough space for the replicated volume and do not contain a volume with a conflicting name (`rprimary-volume-name`) or a snap pool with a conflicting name (`sprprimary-volume-name`).
3. Select the link type used between the two systems.
4. If you want to start replication now:
   a. Select the **Initiate Replication** and **Now** options.
   b. Optionally change the default replication image name. A name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
   c. Continue with step 7.
5. If you want to schedule replication:
   a. Select the **Initiate Replication** and **Scheduled** options.
   b. Set the options:
      - Replication image prefix. Optionally change the default prefix to identify images created by this schedule. The prefix is case sensitive; cannot include a comma, double quote, or backslash; and can have a maximum of 14 bytes.
      - Replication Mode. Specifies whether to replicate a new snapshot of the volume to the remote system, or to replicate the last (most recent existing) snapshot of the volume to the remote system.
      - Replication images to Retain. Select the number of replication images to retain. When the task runs, the retention count is compared with the number of existing replication images:
        - Whether the retention count has been reached or not, a new replication image is created.
        - If the retention count has been reached, the volume's oldest replication image that was created by this schedule and is neither being replicated, nor a current sync point, nor a queued snapshot, is deleted.
        - If there is more than one queued snapshot, only the oldest queued snapshot is retained. It is retained to serve as the source for the next scheduled replication to create a replication image from.

        This setting applies to the primary volume only; for the secondary volume, replication images will accumulate until either the secondary vdisk's space limit is reached or the maximum number of images is reached, after which the oldest image will be deleted as new images are created.
      - Start Schedule. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence. Date must use the format *yyyy-mm-dd*. Time must use the format *hh*:*mm* followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.
      - Recurrence. Specify the interval at which the schedule should run. Set the interval to at least 30 minutes. The default is 30 minutes.
      - Time Constraint. Specify a time range within which the schedule should run.
      - Date Constraint. Specify days when the schedule should run. Ensure that this constraint includes the Start Schedule date.
      - End Schedule. Specify when the schedule should stop running.
   c. Continue with step 7.
6. If you do not want to start or schedule replication, clear the Initiate Replication checkbox. The replication set will still be created and you can replicate the volume at a later time.

7. Click **Apply**. Within a couple of minutes, the replication set is created and the following changes occur in the Configuration View panel:
   - Under the primary vdisk:
     - The selected primary volume changes to a master volume, and is designated as a Primary Volume.
     - If the secondary volume is on a remote system, the secondary volume appears under the primary volume.
     - If a replication was performed, under both the primary volume and the secondary volume a replication image appears.
     - If not already present, the primary volume's snap pool appears.
   - Under the secondary vdisk:
     - The secondary volume appears.
     - If the primary volume is on a remote system, the primary volume appears under the secondary volume.
     - If a replication was performed, under both the primary volume and the secondary volume a replication image appears.
     - If not already present, the secondary volume's snap pool appears.

Replicating a snapshot

If the system is licensed to use remote replication, you can replicate an existing, primary snapshot that is mapped to a host. You can only replicate a snapshot of a volume that is already part of a replication set.

If the selected snapshot hasn't already been replicated to a secondary volume, each replication volume in the replication set is requested to replicate the snapshot data. Only snapshot preserved data is replicated; snapshot modified data is not replicated.

To replicate a snapshot

1. In the Configuration View panel, right-click a snapshot and select **Provisioning > Replicate Snapshot**.
2. In the main panel, optionally change the default replication image name. A name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Initiate Replication**. In a few seconds, the following changes occur in the Configuration View panel:
   - Under both the primary volume and the secondary volume, a replication image appears.

Removing replication from a volume

If the system is licensed to use remote replication and you no longer want to replicate a volume, you can remove its replication set. When a replication set is removed:

- A rollback is automatically performed to the latest available snapshot on the secondary volume to ensure that data is consistent.
- Replication volumes associated with the replication set are converted to master volumes.
- Any replication images associated with the replication volumes are converted to standard snapshots. Snapshots are converted regardless of the number of snapshots allowed by the system's license.
- There is no longer a relationship between the volumes or their snapshots in the two vdisks.

To remove replication from a volume

1. In the Configuration View panel, right-click a local primary volume and select **Provisioning > Remove Replication Set**.
2. In the main panel, click **Remove Replication Set**. A message indicates whether the task succeeded or failed. If it succeeded, the following changes occur in the Configuration View panel:
   - Under the primary vdisk:
     - The primary volume's designation is changed from Primary Volume to Volume

- The secondary volume is removed
- Any replication images are replaced by snapshots

- Under the secondary vdisk:
  - The secondary volume's designation is changed from Secondary Volume to Volume
  - The primary volume is removed
  - Any replication images are replaced by snapshots

NOTE: Normally, if you want to remove a replication set you must select its primary volume. However, if the primary volume is inaccessible, you can set the secondary volume to be the primary volume (as described in Changing the primary volume for a replication set on page 118) and then perform a Remove Replication Set operation.

Suspending replication

If the system is licensed to use remote replication, you can suspend the current replication operation for a selected a replication volume. You must perform this task on the system that owns the secondary volume. Once suspended, the replication must be resumed or aborted to allow the replication volume to resume normal operation.

To suspend replication

1. In the Configuration View panel, right-click a local replication volume and select **Provisioning > Suspend Replication**.
2. In the main panel, click **Suspend Replication**. A message indicates whether the task succeeded or failed.

Resuming replication

If the system is licensed to use remote replication, you can resume a suspended replication operation for a selected replication volume. You must perform this task on the system that owns the secondary volume.

To resume replication

1. In the Configuration View panel, right-click a local replication volume and select **Resume Replication**.
2. In the main panel, click **Resume Replication**. A message indicates whether the task succeeded or failed.

Aborting replication

If the system is licensed to use remote replication, you can abort the current replication operation for the selected replication volume. The current replication may be running or suspended. You must perform this task on the system that owns the secondary volume.

To abort replication

1. In the Configuration View panel, right-click a local replication volume and select **Provisioning > Abort Replication**.
2. In the main panel, click **Abort Replication**. A message indicates whether the task succeeded or failed.

Detaching a secondary volume

When using the replication feature, if you chose to create a replication set's primary and secondary volumes in the primary system, you can perform the initial replication and then physically move the secondary volume's vdisk into the secondary system.

The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume.
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.

c. Stop the secondary volume's vdisk. For details see Stopping a vdisk on page 116.
d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
e. Move the vdisks into the secondary system.

2. In the secondary system:
   a. Start the snap pools' vdisks. For details see Starting a vdisk on page 117.
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see Reattaching a secondary volume on page 117.

Detached volumes remain associated with their replication sets but are not updated with replication data or with replication control information.

NOTE: It is recommended that the vdisk that you are moving contains only secondary volumes and their snap pools. You are allowed to move other volumes along with secondary volumes and their snap pools, but be sure that you are doing so intentionally.

NOTE: If you intend to move a vdisk's drive enclosure and you want to allow I/O to continue to the other enclosures, it is best if it is at the end of the chain of connected enclosures. If the enclosure is in the middle of the chain, the enclosures must be cabled with no single point of failure, so that removing the enclosure does not prevent communication between other enclosures.

To detach a secondary volume

1. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Detach Replication Volume**.
2. In the main panel, click **Detach Replication Volume**. A message indicates whether the task succeeded or failed. When a volume is detached its status is shown as Detached.

Stopping a vdisk

Stopping a vdisk is part of the process for moving a secondary volume into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see Detaching a secondary volume on page 115.
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk.
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system.
2. In the secondary system:
   a. Start the snap pools' vdisks. For details see Starting a vdisk on page 117.
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see Reattaching a secondary volume on page 117.

Before stopping a vdisk, ensure that all secondary volumes that it contains are detached. When a vdisk is stopped:

- The volumes in the vdisk become inaccessible to hosts.
- Its cached data is flushed to disk.
- Removing its disks will not cause the system to report errors or to attempt reconstruction.

NOTE: You cannot stop a vdisk that contains a primary volume.

NOTE: If a secondary volume and its snap pool are in different vdisks, you cannot stop the snap pool's vdisk until you stop the secondary volume's vdisk.

To stop a vdisk

1. In the Configuration View panel, right-click the vdisk and select **Provisioning > Stop Vdisk**.
2. In the main panel, click **Stop Vdisk**. A confirmation prompt appears.
3. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, the stop operation begins. A message indicates whether the task succeeded or failed. If the stop operation succeeds, the vdisk's health is shown as Unknown, its status is shown as STOP, and its subcomponents are no longer displayed in the Configuration View panel.
4. If the stop operation succeeded for the secondary volume's vdisk and for its snap pool's vdisk (if applicable), you can move the disks into the remote system.

Starting a vdisk

Starting a vdisk is part of the process for moving a secondary volume from a primary system into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see Detaching a secondary volume on page 115.
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk. For details see Stopping a vdisk on page 116.
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system.
2. In the secondary system:
   a. Start the snap pools' vdisks.
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see Reattaching a secondary volume on page 117.

To start a vdisk

1. In the Configuration View panel, right-click a stopped vdisk and select **Provisioning > Start Vdisk**.
2. In the main panel, click **Start Vdisk**. A message indicates whether the task succeeded or failed.

NOTE: If the replication set was deleted while the secondary volume's vdisk was stopped, restarting the vdisk will make the set partially reappear. To clean up this remnant, reattach the secondary volume, set it to be the primary volume (by using the Set Replication Primary Volume panel on page 118), and then delete the replication set again.

Reattaching a secondary volume

Reattaching a secondary volume is the last part of the process for moving a secondary volume from a primary system into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see Detaching a secondary volume on page 115.
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk. For details see Stopping a vdisk on page 116.
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system.

2. In the secondary system:
   a. Start the snap pools' vdisks. For details see Starting a vdisk on page 117.
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes.

To reattach a secondary volume

1. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Reattach Replication Volume**.
2. In the main panel, click **Reattach Replication Volume**. A message indicates whether the task succeeded or failed.
   - If the task succeeds, the secondary volume's status changes to "Establishing proxy" while it is establishing the connection to the remote (primary) system in preparation for replication; then the status changes to Online. The replication set is ready to resume replication operations.
   - If the reattach operation fails and says it is unable to get the primary volume's link type, the vdisk that contains the secondary volume may not have completed its startup activities. Wait approximately one minute for these activities to complete, then retry the operation. If this message continues to occur, check the event log to better understand the condition and for an indication of how to correct it.

Exporting a replication image to a snapshot

If the system is licensed to use remote replication, you can export a replication image to a new standard snapshot. For example, you could export a replication image from a secondary volume for use on the remote system. The standard snapshot will reside in the same snap pool, take a snapshot license, and be independent of the primary replication image, which can continue to be used as a sync point. The standard snapshot can be used like any other standard snapshot, and changes to it will not affect the replication image.

The standard snapshot is subject to the snap pool's deletion policies. If the snap pool reaches its critical threshold, the snapshot may be deleted, even if it is mapped. If you want to preserve the standard snapshot's data, you can create a standard volume from the snapshot; see Creating a volume copy on page 67.

NOTE: The export task will not succeed if the resulting snapshot would exceed license limits.

To export a replication image to a snapshot

1. In the Configuration View panel, right-click a replication image and select **Provisioning > Export Snapshot**.
2. In the main panel, optionally change the default name for the snapshot. A snapshot name is case sensitive; cannot already exist in a vdisk; cannot include a comma, double quote, or backslash; and can have a maximum of 20 bytes.
3. Click **Export Snapshot**. A message specifies whether the task succeeded or failed.
4. Click **OK**. If the task succeeds, in the Configuration View panel the snapshot appears under the secondary volume on the remote system.

Changing the primary volume for a replication set

If a replication set's primary system goes offline, you can set the secondary volume to be the primary volume so hosts can access that volume and the replicated data it contains. Scheduled replications can continue on the remote system while the primary system remains offline.

When the secondary volume becomes the primary volume, it only retains the replication images that the primary volume had and deletes any images that the primary volume did not have. Because the secondary volume may not have successfully replicated all the images associated with the primary volume, the secondary volume might have a subset of the primary volume's images.

If the primary system comes back online, you can set its volume to be the primary volume again.

To change the secondary volume to the primary volume

1. On the secondary system, in the Configuration View panel, right-click the secondary volume and select **Provisioning > Set Replication Primary Volume**.
2. In the main panel, select the secondary volume in the list.
3. Click **Set Replication Primary Volume**. A message indicates whether the task succeeded or failed. If it succeeded, in the Configuration View panel the volume's designation changes from Secondary Volume to Primary Volume.

NOTE: The offline primary volume remains designated a Primary Volume.

To change the primary volume back to the original primary volume

1. On the primary system:
   a. Create a standard snapshot (page 65) to preserve the primary volume's last data level.
   b. In the Configuration View panel, right-click the primary volume and select **Provisioning > Set Replication Primary Volume**.
   c. In the main panel, select the primary volume in the list.
   d. Click **Set Replication Primary Volume**. A message indicates whether the task succeeded or failed.
2. On the secondary system:
   a. Replicate the secondary volume (page 112) to synchronize at the last valid common sync point. This will replicate any data changes made in the secondary volume back to the original primary volume.

   NOTE: An administrator can mount/present/map this snapshot and the snapshot taken in step 1 and compare them to verify any discrepancies.

   b. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Set Replication Primary Volume**.
   c. In the main panel, select the primary volume in the list.
   d. Click **Set Replication Primary Volume**. A message indicates whether the task succeeded or failed.
3. On the primary system:
   a. In the Configuration View panel, right-click the primary volume and select **Provisioning > Set Replication Primary Volume**.
   b. In the main panel, select the primary volume in the list.
   c. Click **Set Replication Primary Volume**. A message indicates whether the task succeeded or failed. If it succeeded, in the Configuration View panel the primary volume is designated the Primary Volume and the secondary volume is re-designated the Secondary Volume.

Viewing replication properties, addresses, and images for a volume

In the Configuration View panel, right-click a volume and select **View > Overview**. The Volume Overview table shows:

- As described in Viewing information about a volume on page 92: the capacity and space usage of the volume; the quantity of mappings for the volume; and the quantity of task schedules for the volume
- The quantity of replication addresses for the volume
- The quantity of replication images for the volume

For descriptions of storage-space color codes, see About storage-space color codes on page 31.

Select a component to see more information about it.

Replication properties

For a *local* primary or secondary volume, the Replication Properties for Volume table also shows:

- Name. Replication volume name.
- Serial Number. Replication volume serial number.
- Status. Replication volume status: Replicating, Suspended, Initializing, Inconsistent, Offline, Online, or Establishing proxy. After a secondary volume is reattached it has “Establishing proxy” status while establishing a proxy connection with the remote (primary) system in preparation for replication.
- Status-Reason. More information about the status value, or N/A for Online status.
- Monitor. Interval in seconds at which the primary volume should query the secondary volume.
- Location. Local or Remote.
- Primary Volume Name. Primary volume name. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Serial Number. Primary volume serial number. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Status. Primary volume status: Online, Offline, Conflict, or N/A.
- Maximum Number of Queued Images. Number of replication images to consider when determining the next image to replicate. Used only if the On Collision parameter is set to Oldest.
- Maximum Retry Time (Seconds). Amount of time in seconds that the replication volume should retry a replication operation on any specific image when errors occur. Used only if the On Error parameter is set to Retry.
- On Error. Error policy to invoke when errors occur during the replication process: Retry or Suspend.
- Link Type. Type of ports used to link the primary and secondary volumes: FC or iSCSI.
- On Collision. Collision policy used to determine the next image to replicate when multiple replication images are queued: Newest or Oldest.
- Priority. Priority of the replication process on the replication volume: Low, Medium, or High.
- Connection Status.
  - Not Attempted. Communication has not been attempted to the remote volume.
  - Online. The volumes in the replication set have a valid connection but communication is not currently active.
  - Active. Communication is currently active to the remote volume.
  - Offline. No connection is available to the remote system.
- Connection Time. Date and time of the last communication with the remote volume, or N/A.

Replication addresses

If any remote port addresses are associated with this volume, when you select the Replication Addresses component, the Replication Addresses table shows:

- Connected Ports.
  - For a remote primary or secondary volume, this field shows the IDs of up to two hosts ports in the local system that are connected to the remote system. If two ports are connected but only one is shown, this indicates that a problem is preventing half the available bandwidth from being used.
  - For a local primary or secondary volume, this field shows N/A.
- Remote Address. The address of each host port in the remote system through which the volume is accessible.

Replication images

If any replication images exist for this volume, when you select the Replication Images component, the Replication Images table shows information about each image. For the selected image, the Replication Images table shows:

- Image Serial Number. Replication image serial number.
- Image Name. User-defined name assigned to the primary replication image.
- Snapshot Serial Number. Replication snapshot serial number associated with the image. The replication snapshot is associated with the replication volume specified in the request.
- Snapshot Name. Replication snapshot name associated with the image. For a secondary replication image, this value is not filled in until the replication is completed.
- Creation Date/Time. Date and time when the replication image was created on the replication volume.

Viewing information about a remote primary or secondary volume

In the Configuration View panel, right-click a *remote* primary or secondary volume and select **View > Overview**. The Replication Volume Overview table shows:

- Replication properties for the volume
- The quantity of replication addresses for the volume
- The quantity of replication images for the volume

Select a component to see more information about it.

Replication properties

When you select the Replication component a table shows the volume's replication properties, including the volume's name, serial number, status, status reason, monitor interval, and location (local or remote); primary volume name, serial number, and status; maximum number of queued images, maximum retry time, error policy, collision policy, link type, and priority; and connection status and last connection date/time.

Replication addresses

When you select the Replication Addresses component a table shows:

- Connected Ports.
  - For a remote primary or secondary volume, this field shows the IDs of up to two hosts ports in the local system that are connected to the remote system. If two ports are connected but only one is shown, this indicates that a problem is preventing half the available bandwidth from being used.
  - For a local primary or secondary volume, this field shows N/A.
- Remote Address. The address of each host port in the remote system through which the volume is accessible.

Replication image properties

When you select the Replication Images component a table shows replication image details including the image serial number and name, snapshot serial number and name, and image creation date/time.

Viewing information about a replication image

In the Configuration View panel, right-click a replication image and select **View > Overview**. The Replication Image Overview table shows:

- Replication status properties
- Primary volume snapshot properties
- Secondary volume snapshot properties

Select a component to see more information about it.

Replication status properties

When you select the Status component a table shows the status, progress, start date/time, date/time of last update, date/time the replication was suspended, estimated completion time, elapsed or total replication time (including any suspension time). The panel also shows the replication image's serial number.

Primary volume snapshot properties

If the snapshot is on the local system, when you select the Primary Volume Snapshot component a table shows the:

- Name and serial number of the vdisk containing the snapshot
- Snapshot name, creation date/time, status, and status reason
- Primary volume name
- Snap pool name
- Amounts of total, unique, and shared data associated with the snapshot
- Default and user-specified retention priorities for this type of snapshot
- Snapshot type

If the snapshot is on a remote system, when you select the Primary Volume Snapshot component a table shows the snapshot serial number and creation date/time.

Secondary volume snapshot properties

If the snapshot is on the local system, when you select the Secondary Volume Snapshot component a table shows the:

- Name and serial number of the vdisk containing the snapshot
- Snapshot name, creation date/time, status, and status reason
- Primary volume name
- Snap pool name
- Amounts of total, unique, and shared data associated with the snapshot
- Default and user-specified retention priorities for this type of snapshot
- Snapshot type

If the snapshot is on a remote system, when you select the Secondary Volume Snapshot component a table shows the snapshot serial number and creation date/time.

A SNMP reference

This appendix describes the Simple Network Management Protocol (SNMP) capabilities that 3000 Series storage systems support. This includes standard MIB-II, the FibreAlliance SNMP Management Information Base (MIB) version 2.2 objects, and enterprise traps.

3000 Series storage systems can report their status through SNMP. SNMP provides basic discovery using MIB-II, more detailed status with the FA MIB 2.2, and asynchronous notification using enterprise traps.

SNMP is a widely used network monitoring and control protocol. It is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Data is passed from SNMP agents reporting activity on each network device to the workstation console used to oversee the network. The agents return information contained in a Management Information Base (MIB), which is a data structure that defines what is obtainable from the device and what can be controlled (turned on and off, etc.).

An SNMP object identifier (OID) is a number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using the IETF notation of digits and dots resembling very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.

3000 Series storage systems use SNMPv2c, which improves on SNMPv1 features and uses its community-based security scheme.

Standard MIB-II behavior

MIB-II is implemented to support basic discovery and status.

In the system group, all objects can be read. The contact, name, and location objects can be set.

The system object identifier (`sysObjectID`) is based on the vendor name followed by ".2." and the identifier for the particular product model. For example, the object identifier for 3000 Series storage systems is 1.3.6.1.4.1.11.2.347. System uptime is an offset from the first time this object is read.

In the interfaces group, an internal PPP interface is documented, but it is not reachable from external to the device.

The address translation (at) and external gateway protocol (egp) groups are not supported.

Enterprise traps

Traps can be generated in response to events occurring in the storage system. These events can be selected by severity and by individual event type. A maximum of three SNMP trap destinations can be configured by IP address.

Enterprise event severities are informational, minor, major, and critical. There is a different trap type for each of these severities. The trap format is represented by the enterprise traps MIB, `dhtraps.mib`. Information included is the event ID, the event code type, and a text description generated from the internal event. Equivalent information can also be sent using email or popup alerts to users who are logged in to RAIDar.

The text of the trap MIB is included at the end of this appendix.

FA MIB 2.2 SNMP behavior

The FA MIB 2.2 objects are in compliance with the FibreAlliance MIB v2.2 Specification (FA MIB2.2 Spec). For a full description of this MIB, go to: www.emc.com/microsites/fibrealliance.

FA MIB 2.2 was never formally adopted as a standard, but it is widely implemented and contains many elements useful for storage products. This MIB generally does not reference and integrate with other standard SNMP information; it is implemented under the experimental subtree.

Significant status within the device includes such elements as its temperature and power sensors, the health of its storage elements such as virtual disks, and the failure of any redundant component including an I/O controller. While sensors can be individually queried, for the benefit of network management systems all the above elements are combined into an "overall status" sensor. This is available as the unit status (`connUnitStatus` for the only unit), and a "sensor" in the sensor table.

The revisions of the various components within the device can be requested through SNMP.

The port section is only relevant to products with Fibre Channel host ports.

The event table allows 400 recently-generated events to be requested. Informational, minor, major, or critical event types can be selected; whichever type is selected enables the capture of that type and more severe events. This mechanism is independent of the assignment of events to be generated into traps.

The traps section is not supported. It has been replaced by an ability to configure trap destinations using the CLI or RAIDar. The statistics section is not implemented.

The following table lists the MIB objects, their descriptions and the value set in a 3000 Series storage system. Unless specified otherwise, objects are *not* settable.

Table 11 FA MIB 2.2 objects, descriptions, and values

Object	Description	Value
`RevisionNumber`	Revision number for this MIB	0220
`UNumber`	Number of connectivity units present	1
`SystemURL`	Top-level URL of the device; for example, `http://10.1.2.3`. If a web server is not present on the device, this string is empty in accordance with the FA MIB2.2 Spec.	Default: `http://10.0.0.1`
`StatusChangeTime`	`sysuptime` timestamp of the last status change event, in centiseconds. `sysuptime` starts at 0 when the Storage Controller boots and keeps track of the up time. `statusChangeTime` is updated each time an event occurs.	0 at startup
`ConfigurationChangeTime`	`sysuptime` timestamp of the last configuration change event, in centiseconds. `sysuptime` starts at 0 when the Storage Controller boots and keeps track of the up time. `configurationChangeTime` is updated each time an event occurs.	0 at startup
`ConnUnitTableChangeTime`	`sysuptime` timestamp of the last update to the `connUnitTable` (an entry was either added or deleted), in centiseconds	0 always (entries are not added to or deleted from the `connUnitTable`)
`connUnitTable`	**Includes the following objects as specified by the FA MIB2.2 Spec**	
`connUnitId`	Unique identification for this connectivity unit	Total of 16 bytes comprised of 8 bytes of the node WWN or similar serial number-based identifier (for example, 1000005013b05211) with the trailing 8 bytes equal to zero
`connUnitGlobalId`	Same as `connUnitId`	Same as `connUnitId`

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitType	Type of connectivity unit	storage-subsystem(11)
connUnitNumports	Number of host ports in the connectivity unit	Number of host ports
connUnitState	Overall state of the connectivity unit	online(2) or unknown(1), as appropriate
connUnitStatus	Overall status of the connectivity unit	ok(3), warning(4), failed(5), or unknown(1), as appropriate
connUnitProduct	Connectivity unit vendor's product model name	Model string
connUnitSn	Serial number for this connectivity unit	Serial number string
connUnitUpTime	Number of centiseconds since the last unit initialization	0 at startup
connUnitUrl	Same as systemURL	Same as systemURL
connUnitDomainId	Not used; set to all 1s as specified by the FA MIB2.2 Spec	0xFFFF
connUnitProxyMaster	Stand-alone unit returns yes for this object	yes(3) since this is a stand-alone unit
connUnitPrincipal	Whether this connectivity unit is the principal unit within the group of fabric elements. If this value is not applicable, returns unknown.	unknown(1)
connUnitNumSensors	Number of sensors in the connUnitSensorTable	33
connUnitStatusChangeTime	Same as statusChangeTime	Same as statusChangeTime
connUnitConfiguration ChangeTime	Same as configurationChangeTime	Same as configurationChangeTime
connUnitNumRevs	Number of revisions in the connUnitRevsTable	16
connUnitNumZones	Not supported	0
connUnitModuleId	Not supported	16 bytes of 0s
connUnitName	Settable: Display string containing a name for this connectivity unit	Default: Uninitialized Name
connUnitInfo	Settable: Display string containing information about this connectivity unit	Default: Uninitialized Info
connUnitControl	Not supported	invalid(2) for an SNMP GET operation and not settable through an SNMP SET operation.
connUnitContact	Settable: Contact information for this connectivity unit	Default: Uninitialized Contact
connUnitLocation	Settable: Location information for this connectivity unit	Default: Uninitialized Location
connUnitEventFilter	Defines the event severity that will be logged by this connectivity unit. Settable only through RAIDar.	Default: info(8)

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitNumEvents	Number of events currently in the connUnitEventTable	Varies as the size of the Event Table varies
connUnitMaxEvents	Maximum number of events that can be defined in the connUnitEventTable	400
connUnitEventCurrID	Not supported	0
connUnitRevsTable	**Includes the following objects as specified by the FA MIB2.2 Spec**	
connUnitRevsUnitId	connUnitId of the connectivity unit that contains this revision table	Same as connUnitId
connUnitRevsIndex	Unique value for each connUnitRevsEntry between 1 and connUnitNumRevs	See External details for connUnitRevsTable on page 129
connUnitRevsRevId	Vendor-specific string identifying a revision of a component of the connUnit	String specifying the code version. Reports "Not Installed or Offline" if module information is not available.
connUnitRevsDescription	Description of a component to which the revision corresponds	See External details for connUnitRevsTable on page 129
connUnitSensorTable	**Includes the following objects as specified by the FA MIB2.2 Spec**	
connUnitSensorUnitId	connUnitId of the connectivity unit that contains this sensor table	Same as connUnitId
connUnitSensorIndex	Unique value for each connUnitSensorEntry between 1 and connUnitNumSensors	See External details for connUnitSensorTable on page 130
connUnitSensorName	Textual identification of the sensor intended primarily for operator use	See External details for connUnitSensorTable on page 130
connUnitSensorStatus	Status indicated by the sensor	ok(3), warning(4), or failed(5) as appropriate for FRUs that are present, or other(2) if FRU is not present.
connUnitSensorInfo	Not supported	Empty string
connUnitSensorMessage	Description the sensor status as a message	connUnitSensorName followed by the appropriate sensor reading. Temperatures display in both Celsius and Fahrenheit; for example, CPU Temperature (Controller Module A): 48C 118F). Reports "Not installed" or "Offline" if data is not available.
connUnitSensorType	Type of component being monitored by this sensor	See External details for connUnitSensorTable on page 130
connUnitSensor Characteristic	Characteristics being monitored by this sensor	See External details for connUnitSensorTable on page 130
connUnitPortTable	**Includes the following objects as specified by the FA MIB2.2 Spec**	
connUnitPortUnitId	connUnitId of the connectivity unit that contains this port	Same as connUnitId
connUnitPortIndex	Unique value for each connUnitPortEntry between 1 and connUnitNumPorts	Unique value for each port, between 1 and the number of ports

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitPortType	Port type	not-present(3), or n-port(5) for point-to-point topology, or l-port(6)
connUnitPortFCClassCap	Bit mask that specifies the classes of service capability of this port. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortFCClassOp	Bit mask that specifies the classes of service that are currently operational. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortState	State of the port hardware	unknown(1), online(2), offline(3), bypassed(4)
connUnitPortStatus	Overall protocol status for the port	unknown(1), unused(2), ok(3), warning(4), failure(5), notparticipating(6), initializing(7), bypass(8)
connUnitPortTransmitterType	Technology of the port transceiver	unknown(1) for Fibre Channel ports
connUnitPortModuleType	Module type of the port connector	unknown(1)
connUnitPortWwn	Fibre Channel World Wide Name (WWN) of the port if applicable	WWN octet for the port, or empty string if the port is not present
connUnitPortFCId	Assigned Fibre Channel ID of this port	Fibre Channel ID of the port All bits set to 1 if the Fibre Channel ID is not assigned or if the port is not present
connUnitPortSn	Serial number of the unit (for example, for a GBIC). If this is not applicable, returns an empty string.	Empty string
connUnitPortRevision	Port revision (for example, for a GBIC)	Empty string
connUnitPortVendor	Port vendor (for example, for a GBIC)	Empty string
connUnitPortSpeed	Speed of the port in KByte per second (1 KByte = 1000 Byte)	Port speed in KByte per second, or 0 if the port is not present
connUnitPortControl	Not supported	invalid(2) for an SNMP GET operation and not settable through an SNMP SET operation
connUnitPortName	String describing the addressed port	See External details for connUnitPortTable on page 131
connUnitPortPhysicalNumber	Port number represented on the hardware	Port number represented on the hardware
connUnitPortStatObject	Not supported	0 (No statistics available)
connUnitEventTable	**Includes the following objects as specified by the FA MIB2.2 Spec**	
connUnitEventUnitId	connUnitId of the connectivity unit that contains this port	Same as connUnitId
connUnitEventIndex	Index into the connectivity unit's event buffer, incremented for each event	Starts at 1 every time there is a table reset or the unit's event table reaches its maximum index value

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitEventId	Internal event ID, incremented for each event, ranging between 0 and connUnitMaxEvents	Starts at 0 every time there is a table reset or connUnitMaxEvents is reached
connUnitREventTime	Real time when the event occurred, in the following format: *DDMMYYYY HHMMSS*	0 for logged events that occurred prior to or at startup
connUnitSEventTime	sysuptime timestamp when the event occurred	0 at startup
connUnitEventSeverity	Event severity level	error(5), warning(6) or info(8)
connUnitEventType	Type of this event	As defined in CAPI
connUnitEventObject	Not used	0
connUnitEventDescr	Text description of this event	Formatted event, including relevant parameters or values
connUnitLinkTable	Not supported	N/A
connUnitPortStatFabric Table	Not supported	N/A
connUnitPortStatSCSITable	Not supported	N/A
connUnitPortStatLANTable	Not supported	N/A
SNMP TRAPS	**The following SNMP traps are supported**	
trapMaxClients	Maximum number of trap clients	1
trapClientCount	Number of trap clients currently enabled	1 if traps enabled; 0 if traps not enabled
connUnitEventTrap	This trap is generated each time an event occurs that passes the connUnitEventFilter and the trapRegFilter	N/A
trapRegTable	Includes the following objects per the FA MIB2.2 Spec	
trapRegIpAddress	IP address of a client registered for traps	IP address set through Telnet
trapRegPort	User Datagram Protocol (UDP) port to send traps to for this host	162
trapRegFilter	Settable: Defines the trap severity filter for this trap host. The connUnit will send traps to this host that have a severity level less than or equal to this value.	Default: warning(6)
trapRegRowState	Specifies the state of the row	READ: rowActive(3) if traps are enabled through Telnet; otherwise rowInactive(2) WRITE: Not supported
Enterprise-specific fields	**Includes the following objects**	
cpqSiSysSerialNum	System serial number	For example, 3CL8Y40991
cpqSiSysProductId	System product ID	For example, 481321-001
cpqSiProductName	System product name	For example, DH3000

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
cpqHoMibStatusArray	An array of MIB status structures. Octets 0–3 in block 0 are reserved for systems management and serve as an aggregate of the other MIBs.	Octet 0: 0. Octet 1 (overall status): 0 = Not available; 1 = Unknown/other; 2 = OK/normal; 3 = Degraded/warning; 4 = Failed/critical Octet 2 (system flags): 9 = device is not a server and web-based management is enabled Octet 3 (device type): 14 = enclosure For example, 00.02.09.14 (hex)
cpqHoGUID	Globally unique identifier formed from the product ID and serial number	For example, 4813213CL8Y40991

External details for certain FA MIB 2.2 objects

Tables in this section specify values for certain objects described in Table 11.

External details for connUnitRevsTable

Table 12 connUnitRevsTable index and description values

connUnitRevsIndex	connUnitRevsDescription
1	Firmware revision for Storage Controller (Controller A)
2	Firmware revision for Storage Controller (Controller B)
3	Firmware revision for Memory Controller (Controller A)
4	Firmware revision for Memory Controller (Controller B)
5	Firmware revision for Storage Controller loader (Controller A)
6	Firmware revision for Storage Controller loader (Controller B)
7	Firmware revision for Management Controller (Controller A)
8	Firmware revision for Management Controller (Controller B)
9	Firmware revision for MC loader (Controller A)
10	Firmware revision for MC loader (Controller B)
11	Firmware Revision for Unified CPLD (Controller A)
12	Firmware Revision for Unified CPLD (Controller B)
13	Firmware Revision for Expander (Controller A)
14	Firmware Revision for Expander (Controller B)
15	Hardware Revision for Controller A
16	Hardware Revision for Controller B

External details for connUnitSensorTable

Table 13 connUnitSensorTable index, name, type, and characteristic values

connUnitSensorIndex	connUnitSensorName	connUnitSensorType	connUnitSensor Characteristic
1	CPU Temperature (Controller A)	board(8)	temperature(3)
2	CPU Temperature (Controller B)	board(8)	temperature(3)
3	FPGA Temperature (Controller A)	board(8)	temperature(3)
4	FPGA Temperature (Controller B)	board(8)	temperature(3)
5	Onboard Temperature 1 (Controller A)	board(8)	temperature(3)
6	Onboard Temperature 1 (Controller B)	board(8)	temperature(3)
7	Onboard Temperature 2 (Controller A)	board(8)	temperature(3)
8	Onboard Temperature 2 (Controller B)	board(8)	temperature(3)
9	Capacitor Temperature (Controller A)	board(8)	temperature(3)
10	Capacitor Temperature (Controller B)	board(8)	temperature(3)
11	CM Temperature (Controller A)	enclosure(7)	temperature(3)
12	CM Temperature (Controller B)	enclosure(7)	temperature(3)
13	Power Supply 1 Temperature	enclosure(7)	temperature(3)
14	Power Supply 2 Temperature	enclosure(7)	temperature(3)
15	Capacitor Pack Voltage (Controller A)	board(8)	power(9)
16	Capacitor Pack Voltage (Controller B)	board(8)	power(9)
17	Capacitor Cell 1 Voltage (Controller A)	board(8)	power(9)
18	Capacitor Cell 1 Voltage (Controller B)	board(8)	power(9)
19	Capacitor Cell 2 Voltage (Controller A)	board(8)	power(9)
20	Capacitor Cell 2 Voltage (Controller B)	board(8)	power(9)
21	Capacitor Cell 3 Voltage (Controller A)	board(8)	power(9)
22	Capacitor Cell 3 Voltage (Controller B)	board(8)	power(9)
23	Capacitor Cell 4 Voltage (Controller A)	board(8)	power(9)
24	Capacitor Cell 4 Voltage (Controller B)	board(8)	power(9)
25	Capacitor Charge Current (Controller A)	board(8)	currentValue(6)
26	Capacitor Charge Current (Controller B)	board(8)	currentValue(6)
27	Power Supply 1 Voltage, 12V	power-supply(5)	power(9)
28	Power Supply 1 Voltage, 5V	power-supply(5)	power(9)
29	Power Supply 1 Voltage, 3.3V	power-supply(5)	power(9)
30	Power Supply 2 Voltage, 12V	power-supply(5)	power(9)
31	Power Supply 2 Voltage, 5V	power-supply(5)	power(9)
32	Power Supply 2 Voltage, 3.3V	power-supply(5)	power(9)
33	Overall Status	enclosure(7)	other(2)

External details for connUnitPortTable

Table 14 connUnitPortTable index and name values

connUnitPortIndex	connUnitPortName
1	Host Port 1 (Controller A)
2	Host Port 2 (Controller B)
3	Host Port 1 (Controller A)
4	Host Port 2 (Controller B)

Configuring SNMP event notification in RAIDar

1. Verify that the storage system's SNMP service is enabled; see Changing management interface settings on page 38.
2. Configure and enable SNMP traps; see Configuring SNMP notification on page 39.

SNMP management

You can manage storage devices using SNMP with a network management system such as HP OpenView, HP System Insight Manager (SIM), or HP Instant Support Enterprise Edition (ISEE). See their documentation for information about loading MIBs, configuring events, and viewing and setting group objects.

In order to view and set system group objects, SNMP must be enabled in the storage system; see Changing management interface settings on page 38.

Enterprise trap MIB

The following pages show the source for the enterprise traps MIB, `dhtraps.mib`. This MIB defines the content of the SNMP traps that 3000 Series storage systems generate.

```
-- ------------------------------------------------------
-- Dot Hill Low Cost Array MIB for SNMP Traps
--
-- $Revision: 11692 $
--
-- Copyright 2005 Dot Hill Systems Corp.
-- All rights reserved. Use is subject to license terms.
--
-- ------------------------------------------------------

DHTRAPS-MIB
-- Last edit date: Nov 11th, 2005
DEFINITIONS ::= BEGIN
  IMPORTS
    enterprises
        FROM RFC1155-SMI
    TRAP-TYPE
        FROM RFC-1215
    connUnitEventId, connUnitEventType, connUnitEventDescr
        FROM FCMGMT-MIB;


    --Textual conventions for this MIB

-------------------------------------------------------------------------
    -- formerly Box Hill
    dothill    OBJECT IDENTIFIER ::= { enterprises 347 }
```

```
-- Related traps

    dhEventInfoTrap TRAP-TYPE
        ENTERPRISE dothill
        VARIABLES { connUnitEventId,
                    connUnitEventType,
                    connUnitEventDescr }
        DESCRIPTION
            "An event has been generated by the storage array.
            Recommended severity level (for filtering): info"

        -- Trap annotations are as follows:
        --#TYPE "Informational storage event"
        --#SUMMARY "Informational storage event # %d, type %d, description: %s"
        --#ARGUMENTS {0,1,2}
        --#SEVERITY INFORMATIONAL
        --#TIMEINDEX 6
        ::= 1

    dhEventWarningTrap TRAP-TYPE
        ENTERPRISE dothill
        VARIABLES { connUnitEventId,
                    connUnitEventType,
                    connUnitEventDescr }
        DESCRIPTION
            "An event has been generated by the storage array.
            Recommended severity level (for filtering): warning"

        -- Trap annotations are as follows:
        --#TYPE "Warning storage event"
        --#SUMMARY "Warning storage event # %d, type %d, description: %s"
        --#ARGUMENTS {0,1,2}
        --#SEVERITY MINOR
        --#TIMEINDEX 6
        ::= 2

    dhEventErrorTrap TRAP-TYPE
        ENTERPRISE dothill
        VARIABLES { connUnitEventId,
                    connUnitEventType,
                    connUnitEventDescr }
        DESCRIPTION
            "An event has been generated by the storage array.
            Recommended severity level (for filtering): error"

        -- Trap annotations are as follows:
        --#TYPE "Error storage event"
        --#SUMMARY "Error storage event # %d, type %d, description: %s"
        --#ARGUMENTS {0,1,2}
        --#SEVERITY MAJOR
        --#TIMEINDEX 6
        ::= 3

    dhEventCriticalTrap TRAP-TYPE
        ENTERPRISE dothill
        VARIABLES { connUnitEventId,
                    connUnitEventType,
                    connUnitEventDescr }
```

```
        DESCRIPTION
            "An event has been generated by the storage array.
            Recommended severity level (for filtering): critical"

        -- Trap annotations are as follows:
        --#TYPE "Critical storage event"
        --#SUMMARY "Critical storage event # %d, type %d, description: %s"
        --#ARGUMENTS {0,1,2}
        --#SEVERITY CRITICAL
        --#TIMEINDEX 6
        ::= 4

END
```

B Using FTP to download logs and update firmware

Although RAIDar is the preferred interface for downloading logs, updating firmware, and installing a license, you can also use FTP to do these tasks.

IMPORTANT: Do not attempt to do more than one of the operations in this appendix at the same time. They can interfere with each other and the operations may fail. Specifically, do not try to do more than one firmware update at the same time or try to download system logs while doing a firmware update.

Downloading system logs

To help service personnel diagnose a system problem, you might be asked to provide system log data. You can download this data by accessing the system's FTP interface and running the `get logs` command. When both controllers are online, regardless of operating mode, `get logs` will download a single, compressed zip file that includes:

- User configuration settings from both controllers
- Event logs from both controllers
- SC logs from both controllers
- SC crash dumps from both controllers
- CAPI trace from the controller receiving the command
- MC log from the controller receiving the command
- Controller environment (including data about attached disks, enclosures, and so forth)

It is recommended to use a command-line-based FTP client. A GUI-based FTP client might not work.

To download logs to a file

1. In RAIDar, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers; see Changing network interface settings on page 44.
   b. Verify that the system's FTP service is enabled; see Changing management interface settings on page 38.
   c. Verify that the user you will log in as has permission to use the FTP interface; see Modifying users on page 41.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Enter:

   `ftp` *`controller-network-address`*

   For example:

   `ftp 10.1.0.9`
4. Log in as a user that has permission to use the FTP interface.
5. Enter:

   `get logs` *`filename`***`.zip`**

   where *`filename`* is the file that will contain the logs. It is recommended to choose a filename that identifies the system, controller, and date. For example:

   `get logs Storage2_A_20100124.zip`

   Wait for the message `Operation Complete` to appear.
6. Quit the FTP session.
7. If the problem to diagnose seems specific to user-interface behavior, repeat step 3 through step 6 on the partner controller to collect its unique MC log data.

NOTE: You must uncompress a zip file before you can view the files it contains. To examine diagnostic data, first view `store_yyyy_mm_dd__hh_mm_ss.logs`.

Updating firmware

You can update the versions of firmware in controller modules, expansion modules (in drive enclosures), and disks.

TIP: To ensure success of an online update, select a period of low I/O activity. This helps the update complete as quickly as possible and avoids disruptions to host and applications due to timeouts. Attempting to update a storage system that is processing a large, I/O-intensive batch job will likely cause hosts to lose connectivity with the storage system.

NOTE: If a vdisk is quarantined, firmware update is not permitted due to the risk of losing unwritten data that remains in cache for the vdisk's volumes. Before you can update firmware, you must resolve the problem that is causing the vdisk to be quarantined, as described in Removing a vdisk from quarantine on page 83.

Updating controller-module firmware

A controller enclosure can contain one or two controller modules. In a dual-controller system, both controllers should run the same firmware version. Storage systems in a replication set must run the same firmware version. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

If you have a dual-controller system and the Partner Firmware Update option is enabled, when you update one controller the system automatically updates the partner controller. If Partner Firmware Update is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

Firmware update via FTP is supported from any of the following versions: TS200R021, TS201R014, TS201R015, TS201P004, TS210R016, and TS220R004. From TS100 you must first update to TS201R015 and then to the latest TS230 version.

To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. In RAIDar, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
3. If the storage system has a single controller, stop I/O to vdisks before starting the firmware update.
4. Restart the Management Controller (MC) in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers. For the procedure, see Restarting or shutting down controllers on page 80.
5. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the firmware file to load.
6. Enter:

   `ftp` *`controller-network-address`*

   For example:

   `ftp 10.1.0.9`

7. Log in as an FTP user.
8. Enter:

   put *firmware-file* **flash**

   For example:

   put T230R01-01.bin flash

   △ **CAUTION:** Do not perform a power cycle or controller restart during a firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

   NOTE: If you attempt to load an incompatible firmware version, the message `*** Code Load Fail. Bad format image. ***` is displayed and after a few seconds the FTP prompt is redisplayed. The code is not loaded.

   Firmware update typically takes 10 minutes for a controller having current CPLD firmware, or 20 minutes for a controller having downlevel CPLD firmware. If the controller enclosure has attached drive enclosures, allow additional time for each expansion module (EMP) to be updated. This typically takes 3 minutes for an EMP in each MSA2000 drive enclosure.

   NOTE: If you are using a Windows FTP client, during firmware update a client-side FTP application issue can cause the FTP session to be aborted. If this issue persists try using RAIDar to perform the update, use another client, or use another FTP application.

   If the Storage Controller cannot be updated, the update operation is cancelled. If the FTP prompt does not return, quit the FTP session and log in again. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

   When firmware update on the local controller is complete, the message `Operation Complete` is printed, the FTP session returns to the `ftp>` prompt, and the FTP session to the local MC is closed.

   If PFU is enabled, allow an additional 10–20 minutes for the partner controller to be updated.
9. Quit the FTP session.
10. Clear your web browser's cache, then sign in to RAIDar. If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

    NOTE: After firmware update has completed on both controllers, if the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

Updating expansion-module firmware

A drive enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

Expansion-module firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion module by loading a firmware file obtained from the enclosure vendor.

You can specify to update all expansion modules or only specific expansion modules. If you specify to update all expansion modules and the system contains more than one type of enclosure, the update will be attempted on all enclosures in the system. The update will only succeed for enclosures whose type matches the file, and will fail for enclosures of other types.

To update expansion-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If you want to update all expansion modules, continue with the next step; otherwise, in RAIDar, determine the address of each expansion module to update:
   a. In the Configuration View panel, select a drive enclosure.
   b. In the enclosure properties table, note each EMP's bus ID and target ID values. For example, 0 and 63, and 1 and 63. Bus 0 is the bus that is native to a given controller, while bus 1 is an alternate path through the partner controller. It is recommended to perform update tasks consistently through one controller to avoid confusion.
3. In RAIDar, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
4. If the system has a single controller, stop I/O to vdisks before starting the firmware update.
5. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the firmware file to load.
6. Enter:

   ftp *controller-network-address*

   For example:

   ftp 10.1.0.9
7. Log in as an FTP user.
8. Either:
   - To update all expansion modules, enter:

     put *firmware-file* **encl**
   - To update specific expansion modules, enter:

     put *firmware-file* **encl:***EMP-bus-ID*:*EMP-target-ID*

     For example:

     put S110R01.bin encl:1:63

   △ **CAUTION:** Do not perform a power cycle or controller restart during the firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

   It typically takes 1.5 minutes to update each EMP in a drive enclosure. Wait for a message that the code load has completed.

   NOTE: If the update fails, verify that you specified the correct firmware file and try the update a second time. If it fails again, contact technical support.
9. If you are updating specific expansion modules, repeat step 8 for each remaining expansion module that needs to be updated.
10. Quit the FTP session.
11. Verify that each updated expansion module has the correct firmware version.

Updating disk firmware

You can update disk firmware by loading a firmware file obtained from your reseller.

A dual-ported disk can be updated from either controller. A single-ported disk that is in a vdisk or is a dedicated spare for a vdisk must be updated from the controller that owns the vdisk. Attempting to update a single-ported disk from the non-owning controller will not cause any change to the disk.

NOTE: Disks of the same model in the storage system must have the same firmware revision.

You can specify to update all disks or only specific disks. If you specify to update all disks and the system contains more than one type of disk, the update will be attempted on all disks in the system. The update will only succeed for disks whose type matches the file, and will fail for disks of other types.

To prepare for update

1. Obtain the appropriate firmware file and download it to your computer or network.
2. Check the disk manufacturer's documentation to determine whether disks must be power cycled after firmware update.
3. If you want to update all disks of the type that the firmware applies to, continue with the next step; otherwise, in RAIDar, for each disk to update:
   a. Determine the enclosure number and slot number of the disk.
   b. If the disk is associated with a vdisk and is single ported, determine which controller owns the vdisk.
4. In RAIDar, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
5. Stop I/O to the storage system. During the update all volumes will be temporarily inaccessible to hosts. If I/O is not stopped, mapped hosts will report I/O errors. Volume access is restored after the update completes.

To update disk firmware

1. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the firmware file to load.
2. Enter:

   ftp *controller-network-address*

   For example:

   ftp 10.1.0.9
3. Log in as an FTP user.
4. Either:
   - To update all disks of the type that the firmware applies to, enter:

     put *firmware-file* **disk**
   - To update specific disks, enter:

     put *firmware-file* **disk:***enclosure-ID*:*slot-number*

     For example:

     put *firmware-file* **disk:1:11**

△ **CAUTION:** Do not power cycle enclosures or restart a controller during the firmware update. If the update is interrupted or there is a power failure, the disk might become inoperative. If this occurs, contact technical support.

It typically takes several minutes for the firmware to load. Wait for a message that the update has succeeded.

NOTE: If the update fails, verify that you specified the correct firmware file and try the update a second time. If it fails again, contact technical support.

5. If you are updating specific disks, repeat step 4 for each remaining disk to update.
6. Quit the FTP session.
7. If the updated disks must be power cycled:
   a. Shut down both controllers by using RAIDar.
   b. Power cycle all enclosures as described in your product's setup guide.

NOTE: If you loaded firmware to a Seagate 750-Gbyte Barracuda ES SATA drive, after spin-up it will be busy for about 50 seconds completing its update. Then it will be ready for host I/O.

8. Verify that each disk has the correct firmware revision.

Installing a license file

1. Ensure that the license file is saved to a network location that the storage system can access.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the license file to load.
3. Log in to the controller enclosure that the file was generated for:

   ftp *controller-network-address*

   For example:

   ftp 10.1.0.9
4. Log in as an FTP user.
5. Enter:

   put *license-file* **license**

   For example:

   put certificate.txt license

   A message confirms whether installation succeeded or failed. If installation succeeds, licensing changes take effect immediately.

C Using SMI-S

This appendix provides information for network administrators who are managing the 3000 Series from a storage management application through the Storage Management Initiative Specification (SMI-S). SMI-S is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices.

SMI-S overview

SMI-S replaces multiple disparate managed object models, protocols, and transports with a single object-oriented model for each type of component in a storage network. The specification was created by SNIA to standardize storage management solutions. SMI-S enables management applications to support storage devices from multiple vendors quickly and reliably because they are no longer proprietary. SMI-S detects and manages storage elements by type, not by vendor.

Key components

The key SMI-S components are:

- Web-based Enterprise Management (WBEM)
- Common Information Model (CIM)
- Service Location Protocol (SLP)

WBEM

WBEM is a set of management and internet standard technologies developed to unify the management of enterprise computing environments. WBEM includes the following specifications:

- xmlCIM: defines XML elements, conforming to Document Type Definition (DTD), which can be used to represent CIM classes and instances
- CIM Operations over HTTP: defines a mapping of CIM operations onto HTTP; used as a transport mechanism

CIM

CIM, the data model for WBEM, provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. SMI-S is the interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. The standard language used to define elements of CIM is Managed Object Format (MOF). Unified Modeling Language (UML) is used to create a graphical representation (using boxes and lines) of objects and relationships.

SLP

SLP enables computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks

Profiles

SMI-S is organized around profiles, which describe objects relevant for a class of storage subsystem. SMI-S includes profiles for arrays, Fibre Channel host bus adapters (HBAs), Fibre Channel switches, and tape libraries. Other storage devices are expected to be added in the future. Profiles are registered with the CIM server and advertised to clients using SLP. HP SIM determines which profiles it intends to manage, and then uses the CIM model to discover the actual configurations and capabilities.

SMI-S implementation

SMI-S is implemented with the following components:

- CIM server (called a CIM Object Manager or CIMOM), which listens for WBEM requests (CIM operations over HTTP) from a CIM client, and responds.
- CIM provider, which actually communicates to a particular type of managed resource (for example, HP MSA arrays), and provides the CIMOM with information about them. In theory, providers for multiple types of devices (for example, HP MSA arrays and Brocade switches) can be plugged into the same CIMOM. However, in practice, all storage vendors provide the CIMOM and a single provider together, and they do not co-exist well with solutions from other vendors.

These components may be provided in several different ways:

- Embedded agent: The hardware device has an embedded SMI-S agent. No other installation of software is required to enable management of the device.
- SMI solution: The hardware or software ships with an agent that is installed on a host. The agent needs to connect to the device and obtain unique identifying information.

About the 3000 Series SMI-S provider

The 3000 Series SMI-S provider is a full-fledged embedded provider implemented in the firmware. It provides an industry-standard WBEM-based management framework. SMI-S clients can interact with this embedded provider directly and do not need an intermediate proxy provider.

NOTE: Active management features such as RAID provisioning are not supported in this release.

The embedded CIMOM listens to SMI-S queries from the clients only on port 5989 and requires that the credentials be provided for all queries. This provider implementation complies with the SNIA SMI-S specification version 1.3.0.

The namespace details are given below.

- Implementation Namespace - `root/hpq`
- Interop Namespace - `root/interop`

The embedded provider set includes the following providers:

- Instance Provider
- Association Provider
- Method Provider
- Indication Provider

The embedded provider supports the following CIM operations:

- getClass
- enumerateClasses
- enumerateClassNames
- getInstance
- enumerateInstances
- enumerateInstaneceNames
- associators
- associatorNames
- references
- referenceNames
- invokeMethod

SMI-S profiles

Table 15 Supported SMI-S profiles

Profile/Subprofile	Description
Array	Describes RAID array systems. It provides a high-level overview of the array system.
Block Services	Defines a standard expression of existing storage capacity, the assignment of capacity to Storage Pools, and allocation of capacity to be used by external devices or applications.
Physical Package	Models information about a storage system's physical package and optionally about internal sub-packages.
Health	Defines the general mechanisms used in expressing health in SMI-S.
Server	Defines the capabilities of a CIM object manager based on the communication mechanisms that it supports.
FC Target Ports	Models the Fibre Channel specific aspects of a target storage system.
SAS Target Ports	Models the SAS specific aspects of a target storage system.
iSCSI Target Ports	Models the iSCSI specific aspects of a target storage system.
Access Points	Provides addresses of remote access points for management services.
Fan	Specializes the DMTF Fan profile by adding indications.
Power Supply	Specializes the DMTF Power Supply profile by adding indications.
Profile Registration	Models the profiles registered in the object manager and associations between registration classes and domain classes implementing the profile.
Software	Models software or firmware installed on the system.
Masking and Mapping	Models device mapping and masking abilities for SCSI systems.
Disk Drive Lite	Models disk drive devices.
Extent Composition	Provides an abstraction of how it virtualizes exposable block storage elements from the underlying Primordial storage pool.
Location	Models the location details of product and its sub-components.
Sensors	Specializes the DMTF Sensors profile.
Software Inventory	Models installed and available software and firmware.
Storage Enclosure	Describes an enclosure that contains storage elements (e.g., disk or tape drives) and enclosure elements (e.g., fans and power supplies).
Multiple Computer System	Models multiple systems that cooperate to present a "virtual" computer system with additional capabilities or redundancy.

CIM Alerts

Table 16 CIM Alert indication events

FRU/Event category	Corresponding SMI-S class	Operational status values that would trigger alert conditions
Controller	DHS_Controller	Down, Not Installed, OK
Hard Disk Drive	DHS_DiskDrive	Unknown, Missing, Error, Degraded, OK
Fan	DHS_PSUFan	Error, Stopped, OK
Power Supply	DHS_PSU	Unknown, Error, Other, Stressed, Degraded, OK
Temperature Sensor	DHS_OverallTempSensor	Unknown, Error, Other, Non-Recoverable Error, Degraded, OK
Battery/Super Cap	DHS_SuperCap	Unknown, Error, OK
FC Port	DHS_FCPort	Stopped, OK
SAS Port	DHS_SASTargetPort	Stopped, OK
iSCSI Port	DHS_ISCSIEthernetPort	Stopped, OK

NOTE: There is no support for Life Cycle indications in this release.

SMI-S configuration

In the default SMI-S configuration:

- The SMI-S protocol is turned on.
- The SMI-S interface is enabled for the `manage` user.

The following table lists the CLI commands relevant to the SMI-S protocol:

Action	CLI command
Enable the SMI-S protocol	`set protocols smis enabled`
Disable the SMI-S protocol	`set protocols smis disabled`
See the current status	`show protocols`

To configure the SMI-S interface for other users:

1. Log in as `manage`
2. If the user does not already exist, create one using this command:
   `create user level manage` *`username`*
3. Type this command:
   `set user` *`username`* `interfaces wbi,cli,smis,ftp`

Frequently asked questions

What is an embedded SMI-S array provider?

The embedded SMI-S array provider provides an implementation of SMI-S 1.3 using `cim-xml` over HTTPS. SMI-enabled management clients such as HP SIM or HP Storage Essentials can perform storage management tasks such as monitoring, configuring or event-management. The provider supports the Array and Server profiles with additional (or supporting subprofiles). The Server profile provides a mechanism to tell the client how to connect and use the embedded provider. The Array profile has the following supporting profiles and subprofiles:

- Array profile
- Block Services profile
- Physical Package
- Health profile
- Multiple Computer Systems subprofile
- Masking and Mapping subprofile
- FC Target Ports subprofile (or iSCSI Target Ports or SAS Target Ports)
- Disk Drive Lite subprofile
- Extent Composition subprofile (starting in TS210)
- Storage Enclosure profile
- Fan profile
- Power Supply profile
- Sensors profile
- Access Points subprofile
- Location profile
- Software Inventory profile
- Software subprofile
- Block Server Performance subprofile (starting in TS230)
- Copy Services and Replication Services subprofile (in a future release)
- CIM Alert indications are supported.
- SLP (Service Location Protocol v2) is supported.
- HTTPS (using SSL encryption) is supported on default port 5989. HTTP is optional on default `http` port 5988.

How do I test SMI-S?

Use an SMI-S certified client for SMI-S 1.3. HP has clients such as HP SIM and HP Storage Essentials. Other common clients are StorageIM, IBM Tivoli, EMC CommandCenter and CA Unicenter. Common WBEM CLI clients are Pegasus `cimcli` and Sblim's `wbemcli`.

Testing also employs a Java Swing GUI called CIM Browser. To certify that the array provider is SMI-S 1.3 compliant, SNIA requires that the providers pass the Conformance Test Program (CTP) tests.

What storage arrays are supported?

Each 3000 Series is supported, including FC, iSCSI, SAS and Hybrid platforms. The classes for Dot Hill are DHS_XXX. The device namespace for Dot Hill is `/root/dhs`.

What's new in this release?

SMI-S 1.3 Array Provider support introduced in T230 (passes 100% CTP 1.3 tests):

- Support for Block Server Performance subprofile
- 20x-30x performance improvements
- HP SIM 6.3 subscribe to WBEM events functionality is supported (TS230 and above)
- Dot Hill AssuredSAN products now support SMI-S
- Fixed removal of indication subscription
- Fixed: Performance of associator commands is slower than the previous provider.
- Fixed: Memory leak causes SMI-S to restart.
- Fixed: Value/ValueMaps are not implemented via getClass.

TS210 support for SMI-S 1.3 Array Provider (passed 85% of CTP 1.3 tests):

- Support for LUN masking and mapping extrinsic methods (ExposePaths, HidePaths, CreateStorageHardwareID, DeleteStorageHardwareID)
- SFCB v1.3.7 CIMOM with v2.22.1 MOFs
- Support for Server profile
- Fixed: Property lists do not return correct list.

TS200/201 support for SMI-S 1.3 Array Provider (passed 65% of CTP 1.3 tests):

- Alert Indications with events sent back to the client using HTTP.
- Support for Extent Composition subprofile
- Support for iSCSI and SAS Target Port subprofiles
- Support for Masking and Mapping subprofile (monitor only)
- SLP v2 Discovery
- Performance Improvement
- SFCB v1.3.7 CIMOM with v2.22.1 MOFs

TS100 (February 2010) - SMI-S 1.3 Array Provider:

- SFCB v1.3.5 CIMOM with v2.22.1 MOFs

What is the architecture?

The architecture requirements for the embedded SMI-S Array provider are to work within the MC architecture, use limited disk space, use limited memory resources and be as fast as a proxy provider running on a server. The provider is an MC application and works by making MC CLI requests. An SMI-S cache caches these requests for 30 to 60 seconds. The disk space used is about 3 MB without qualifiers and 8 MB with qualifiers. The CIMOM (Common Information Model Object Manager) used is the open source SFCB (Small Footprint CIM Broker) CIMOM.

SFCB is a lightweight CIM daemon that responds to CIM client requests and supports the standard CIM XML over `http/https` protocol. The provider is a CMPI (Common Management Protocol Interface) provider and uses this interface. To reduce the memory footprint, a third-party package called CIMPLE (www.simplewbem.org) is used. For more information on SFCB go to sblim.cvs.sourceforge.net/sblim/sfcb/README?view=markup.

What CIM operations are supported?

SFCB provides a full set of CIM operations including GetClass, ModifyClass, CreateClass, DeleteClass, EnumerateClasses, EnumerateClassNames, GetInstance, DeleteInstance, CreateInstance, ModifyInstance, EnumerateInstances, EnumerateInstanceNames, InvokeMethod (MethodCall), ExecQuery, Associators, AssociatorNames, References, ReferenceNames, GetQualifier, SetQualifier, DeleteQualifier, EnumerateQualifiers, GetProperty and SetProperty.

Is the product CTP-certified?

We are working towards being CTP 1.3 certified and may pass the CTP 1.3 tests at the time TS230 is released.

Troubleshooting

Problem: Can't connect to the embedded SMI-S Array provider
Cause: SMI-S protocol is not enabled
Solution: Log in to the array as `manage` and type: `set protocol smis enabled`

Problem: HTTP Error (Invalid username/password or 401 Unauthorized)
Cause: User preferences are configurable for each user on the storage array.
Solution: Check that the user has access to the `smis` interface and set the user preferences to support the `smis` interface, if necessary. See SMI-S configuration on page 144 for instructions on how to add users. Also verify the supplied credentials.

Problem: Unable to connect via HTTP on port 5988
Cause: SMI-S Array provider only supports HTTPS (Secure Socket Layer) communication on port 5989.
Solution: Contact technical support for instructions

Problem: Want to connect securely as user name `my_xxxx`
Cause: Need to add user
Solution: Log in to the array as `manage`. Type `create user level manage my_xxxuser` and then type `set user my_xxxuser interfaces wbi,cli,smis`

Problem: Can't discover via SLP
Cause: SLP multicast has limited range (known as hops)
Solution: Move the client closer to the array or set up a SLP DA server or using unicast requests.

Problem: I can't determine if SMI-S is running
Cause: Initial troubleshooting
Solution: Install wbemcli on a Linux system by typing `apt-get install wbemcli`.
Type `wbemcli -nl -t -noverify ein 'https://manage:!manage@:5989/root/hpq:cim_computersystem'`

Definitions

SMI-S: SNIA's Storage Management Initiative Specification

Recipe: Pseudo-client code added to the SMI-S specification to demonstrate usage of methods and associations.

Intrinsic Methods: Methods inherited from CIM and present in all classes such as getclass, createinstance, enumerateinstances and associatorNames.

Extrinsic Methods: Methods which are particular to a specific class.

Block Server Performance subprofile

The implementation of the block server performance subprofile is split into two parts (phase 1 and phase 2). Phase 1 will implement the CIM_XXXStatisticalData classes and their associations. Phase 2 will implement the GetStatisticsCollection, CreateManifestCollection, AddOrModifyManifest and RemoveManifest methods.

LUN Masking and Mapping operations

The implementation of the Masking and Mapping subprofile's extrinsic methods allows CIM clients to create LUNs by mapping volumes to logical ports. The ExposePaths method is fully implemented and simplifies this operation to 1 step. The CreateStorageHardwareID and DeleteStorageHardwareID methods all CIM clients to create and remove hosts.

Alert Indications

The implementation of alert indications allow a subscribing CIM client to receive events such as FC cable connects, Power Supply events, Fan events, Temperature Sensor events and Disk Drive events.

Full provisioning

We currently do not have a `create vdisk` implementation in the provider. Full provisioning will be modeled in the provider by the Block Services and Masking & Mapping subprofiles.

Replication support

We currently do not have a replication implementation in the provider. Replication will be modeled in the provider by the Copy Services and Replication Services subprofiles in a SMI-S 1.5 provider.

What is the codebase for the CIM clients?

CTP uses the WBEMSolutions WSI J Server v1.2.1 (Java) client

HP SIM uses the Pegasus Java Client

Microsoft System Center uses a Microsoft WMI client

CIM Browser uses the Sblim CIM Client v2.x (Java) client which supports JSR 48

EMC CommandCenter and `cimcli` uses the Pegasus (C++) client

Glossary

CAPI	Configuration Application Programming Interface. The proprietary protocol used for communication between the Storage Controller and the Management Controller in a controller module. CAPI is always enabled.
CHAP	Challenge-Handshake Authentication Protocol.
chunk size	The amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk.
compatible disk	A disk that has enough capacity to replace a failed disk and is the same type (SAS or SATA).
dedicated spare	A disk that is reserved for use by a specific vdisk to replace a failed disk. See compatible disk.
default mapping	Host-access settings that are configured when a volume is created, and that apply to all hosts that are not explicitly mapped to that volume using different settings. See also explicit mapping and masking.
drive spin down (DSD)	A power-saving feature that monitors disk activity in the storage system and spins down inactive SAS and SATA disks, based on user-selectable policies.
dual-port disk	A disk that is connected to both controllers so its data path is fault-tolerant.
dynamic spare	An available compatible disk that is automatically assigned, if the dynamic spares option is enabled, to replace a failed disk in a redundant vdisk. See compatible disk.
EC	Expander Controller. The processor (located in the SAS expander in each controller module and expansion module) that controls the SAS expander and provides SES functionality. See also EMP.
EMP	Enclosure management processor. An EC subsystem that provides SES data such as temperature, power supply and fan status, and the presence or absence of disks.
explicit mapping	Access settings for a host to a volume that override the volume's default mapping. See also default mapping and masking.
FC	Fibre Channel interface protocol.
global spare	A disk that is reserved for use by any redundant vdisk to replace a failed disk. See compatible disk.
host	An external port that the storage system is attached to. The external port may be a port in an I/O adapter in a server, or a port in a network switch.
image ID	A globally unique serial number that identifies the point-in-time image source for a volume. All volumes that have identical image IDs have identical data content, whether they be snapshots or stand-alone volumes.
IQN	iSCSI Qualified Name.
iSCSI	Internet SCSI interface protocol.
iSNS	Internet Storage Name Service.
jumbo frame	In an iSCSI network, a frame that can contain 9000 bytes for large data transfers. A normal frame can contain 1500 bytes.
leftover	The state of a disk that has been automatically excluded from a vdisk, and is no longer needed by the vdisk after the vdisk is reconstructed.
loop	Fibre Channel Arbitrated Loop (FC-AL) topology.
masking	Volume-mapping settings that specify no access to that volume by hosts. See also default mapping and explicit mapping.
master volume	A volume that is enabled for snapshots and has an associated snap pool.

MC	Management Controller. The processor (located in a controller module) that is responsible for human-computer interface and computer-computer interface functions, and interacts with the SC.
metadata	Data in the first sectors of a disk drive that stores all disk, vdisk, and volume specific information including vdisk membership or spare identification, vdisk ownership, volumes and snapshots in the vdisk, host mapping of volumes, and results of the last media scrub.
network port	The Ethernet port on a controller module through which its Management Controller is connected to the network.
point-to-point	Fibre Channel Point-to-Point topology.
primary volume	The volume that is the source of data in a replication set and that can be mapped to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The primary volume exists in a primary vdisk in the primary (or local) storage system.
proxy volume	A virtual volume in the local system that represents a volume in a remote system. Proxy volumes are used internally by the controllers to perform actions such as transferring replication data.
remote replication	Asynchronous (batch) replication of block-level data from a volume in a primary system to a volume in one or more secondary systems by creating a replication snapshot of the primary volume and copying the snapshot data to the secondary systems via Fibre Channel or iSCSI links. The capability to perform remote replication is a licensed feature (AssuredRemote).
replication image	A conceptual term for replication snapshots that have the same image ID in primary and secondary systems. These synchronized snapshots contain identical data and can be used for disaster recovery.
replication set	Associated primary and secondary volumes that are enabled for replication and that typically reside in two physically or geographically separate storage systems. See primary volume and secondary volume.
replication snapshot	A special type of snapshot, created by the remote replication feature, that preserves the state of data of a replication set's primary volume as it existed when the snapshot was created. For a primary volume, the replication process creates a replication snapshot on both the primary system and, when the replication of primary-volume data to the secondary volume is complete, on the secondary system. Replication snapshots are unmappable and are not counted toward a license limit, although they are counted toward the system's maximum number of volumes. A replication snapshot can be exported to a regular, licensed snapshot. See also replication sync point.
replication sync point	The state of a replication snapshot whose corresponding primary or secondary snapshot exists and contains identical data. For a replication set, four types of sync point are identified: the only replication snapshot that is copy-complete on any secondary system is the "only sync point"; the latest replication snapshot that is copy-complete on any secondary system is the "current sync point"; the latest replication snapshot that is copy-complete on all secondary systems is a "common sync point"; a common sync point that has been superseded by a new common sync point is an "old common sync point."
SAS	Serial Attached SCSI interface protocol or disk-drive architecture.
SATA	Serial ATA disk-drive architecture.
SC	Storage Controller. The processor (located in a controller module) that is responsible for RAID controller functions. The SC is also referred to as the RAID controller.
secondary volume	The volume that is the destination for data in a replication set and that is not accessible to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The secondary volume exists in a secondary vdisk in a secondary (or remote) storage system. The contents of a secondary volume are in a constant state of flux and are not in a consistent state while a replication is in process. Only snapshots that are associated with a secondary volume are data consistent.

secret	For use with CHAP, a password that is shared between an initiator and a target to enable authentication.
SES	SCSI Enclosure Services.
single-port disk	A disk that is connected to both controllers so its data path is not fault-tolerant. A single-port disk's type is shown as SAS-S or SATA-S.
snap pool	A volume that stores data that is specific to snapshots of an associated master volume, including copy-on-write data and data written explicitly to the snapshots. A snap pool cannot be mapped.
snapshot	A "virtual" volume that preserves the state of a master volume's data as it existed when the snapshot was created. Data associated with a snapshot is recorded in both the master volume and in its associated snap pool. A snapshot can be mapped and written to. The capability to create snapshots is a licensed feature (AssuredSnap). Snapshots that can be mapped to hosts are counted against the snapshot-license limit, whereas transient and unmappable snapshots are not.
SSD	Solid-state drive.
ULP	Unified LUN Presentation. A RAID controller feature that enables a host to access mapped volumes through any controller host port. ULP incorporates Asymmetric Logical Unit Access (ALUA) extensions.
unwritable cache data	Cache data that has not been written to disk and is associated with a volume that no longer exists or whose disks are not online. If the data is needed, the volume's disks must be brought online. If the data is not needed it can be cleared, in which case it will be lost and data will differ between the host and disk. Unwritable cache is also called orphan data.
vdisk	A "virtual" disk comprising the capacity of one or more disks. The number of disks that a vdisk can contain is determined by its RAID level.
volume	A portion of the capacity of a vdisk that can be presented as a storage device to a host.
volume copy	An independent copy of the data in a volume. The capability to create volume copies is a licensed feature (AssuredCopy) that makes use of snapshot functionality.
WWN	World Wide Name. A globally unique 64-bit number that identifies a node process or node port.
WWNN	World Wide Node Name. A globally unique 64-bit number that identifies a node process.
WWPN	World Wide Port Name. A globally unique 64-bit number that identifies a node port.

Index

Symbols

* (asterisk) in option name 16

A

ALUA 22
array
  See system
asterisk (*) in option name 16
audience 13

B

base for size representations 30
browser
  buttons to avoid 16
  setup 15
bytes versus characters 30

C

cache
  configuring auto-write-through triggers and behaviors 48
  configuring host access to 47
  configuring system settings 47
  configuring volume settings 52
CHAP
  add or modify records 72
  configure for iSCSI hosts 72
  configuring 36, 43
  delete records 72
  overview 20
characters versus bytes 30
color codes for storage space 31
CompactFlash properties 102
configuration
  browser 15
  first-time 15
  system limits 88
Configuration View component icons 31
Configuration View panel, using 16
Configuration Wizard
  using 33
connection mode
  configuring FC 36, 42
controller module properties 100
controllers
  restarting or shutting down 80
  using FTP to update firmware 136
  using WBI to update firmware 75
conventions
  document 14
Coordinated Universal Time (UTC) 30
current owner 51

D

date and time
  about 30
  configuring 42
debug data, saving to a file 78
debug logs
  downloading 135
dedicated spare 19
dedicated spares
  adding and removing 50
default mapping 21
DHCP
  configuring 44
  configuring with Configuration Wizard 33
disk
  properties 87
  state (how used) values 92
disk channels
  rescanning 79
disk metadata
  clearing 79
disk properties 91, 99
disk settings
  configuring 45
disks
  configure SMART 45
  configure spin down for available and global-spare 45
  configuring background scrub 49
  schedule spin down for all 46
  show data transfer rate 99
  using FTP to update firmware 139
  using WBI to update firmware 77
document
  conventions 14
  prerequisite knowledge 13
  related documentation 13
drive spin down
  configure for a vdisk 51
  configure for available and global-spare disks 45
  schedule for all disks 46
dynamic spare 19
dynamic spares
  configuring 45

E

EMP polling rate
  configuring 46
enclosure
  properties 87
  viewing information about 98
enclosure properties 98

event log
viewing 88
event notification
configuring email settings 39
configuring SNMP settings 39
configuring with Configuration Wizard 35
sending a test message 81
event severity icons 88
expansion module properties 102
expansion port properties 101
explicit mapping 21

F

firmware
using FTP to update controller module 136
using FTP to update disk drive 139
using FTP to update expansion module 137
using WBI to update controller module 75
using WBI to update disk 77
using WBI to update expansion module 76
versions 88
firmware update, partner
configuring 48
FTP
downloading system logs 135
updating controller module firmware 136
updating disk drive firmware 139
updating expansion module firmware 137

G

global spare 19
global spares
adding and removing 58

H

hardware
versions 88
help
displaying online 17
using the help window 17
host
adding 70
changing mappings 71
changing name 70
properties 97
viewing information about 97
host access to cache
configuring 47
host mapping properties 98
host port properties 101
host ports
check links in local system 85
check links to remote system 85
configuring 42
configuring with Configuration Wizard 35
resetting 78
hosts
about 20
removing 70
viewing information about all 97

I

I/O module properties 102
icon
WBI communication status 16
icons
storage-system component 31
icons, event severity 88
In port properties 102
iSCSI host security 20
iSCSI IP version
configuring 36, 43
iSNS
configuring 36, 43

J

jumbo frames
configuring 36, 43

L

leftover disk 79
licensed features
managing 37
remote replication 105
snapshot 24
status 88
using FTP to install license file 140
VDS and VSS providers 28
volume copy 26
link rate adjustment 99
link speed
configuring FC 35, 42
configuring iSCSI 36, 43
links
check between controllers in local system 85
check between local and remote systems 85
log data, saving to a file 78
logs
downloading debug 135
loop IDs
configuring FC 36, 42
LUNs
configuring response to missing 47

M

management interface services
configuring 38
configuring with Configuration Wizard 34
mapping volumes
See volume mapping
masked volume 21
master volumes
about 24
maximum physical and logical entities supported 88

metadata
clearing disk 79
MIB
See SNMP
missing LUN response
configuring 47
modified snapshot data, deleting
about 25

N

network port 33
network port properties 101
network ports
configuring 44
configuring with Configuration Wizard 33
NTP
about 30
configuring 42

O

Out port properties 101, 102

P

partner firmware update
configuring 48
passwords
See users
policies and thresholds, snap-pool 96
power supply properties 100
preferred owner 51
prerequisite knowledge 13
primary volume
changing for a replication set 118
priority
configuring utility 49
provisioning
first-time 15
Provisioning Wizard
using to create a vdisk with volumes and mappings 55

Q

quarantined vdisk 83

R

RAID levels
about 28
RAIDar Storage Management Utility
See WBI
read-ahead caching
optimizing 23
related documentation 13
remote replication
about 105
remote systems
about managing 24
adding 50
check links from local system 85
removing 50
viewing information about 103
replication disaster recovery 118
replication image
primary snapshot properties 122
replication status properties 122
secondary snapshot properties 122
viewing information about 121
replication set
changing the primary volume 118
detaching a secondary volume 115
reattaching a secondary volume 117
Replication Setup Wizard
using to set up replication for a volume or snapshot 110
replication snapshot size 106
replication volume
viewing information about a remote primary or secondary 121
rescan disk channels 79
restarting controllers 80
restore the system's default configuration settings 79
revert volume data
See roll back volume data
roll back volume data
about 25

S

schedule
deleting 73
modifying 72
properties 88, 95
scheduling
snapshot 65
snapshot reset 66
volume copy 67
scrub
configuring background disk 49
configuring background vdisk 48
`SCSI MODE SELECT` command
configuring handling of 47
`SCSI SYNCHRONIZE CACHE` command
configuring handling of 47
secondary volume
detaching 115
reattaching 117
selective storage presentation
See volume mapping
shared data (snapshot) 94
shutting down controllers 80
sign out, auto
setting user 40, 41
viewing remaining time 16
signing in to the WBI 15
signing out of the WBI 16
single-controller system
data protection tips 32

size representations
about 30
replication snapshot 106
SMART
configuring 45
snap data 94
snap pool
about 24
creating 69
expanding 84
properties 87, 92, 96
thresholds and policies 96
viewing information about 96
snap pools
deleting 70
renaming 53
snapshot
creating 65
exporting replication image to 118
preparing replication by using the Replication Setup Wizard 110
properties 88, 94, 97
replicating 114
resetting to current data in master volume 66
viewing information about 94
snapshot mapping properties 95
snapshots
about 24
creating for multiple volumes 64
deleting 65
renaming 53
SNMP
configuring traps 131
enterprise trap MIB 131
enterprise traps 123
external details for connUnitPortTable 131
external details for connUnitRevsTable 129
external details for connUnitSensorTable 130
FA MIB 2.2 behavior 123
FA MIB 2.2 objects, descriptions, and values 124
management 131
MIB-II behavior 123
overview 123
setting event notification 131
sorting a table 16
spares
about 19
See also dedicated spare, dynamic spare, and global spare
storage system
See system
synchronize-cache mode
configuring 47
system
configuration limits 88
data protection tips for a single-controller 32
properties 87
restore default configuration settings 79
viewing event log 88
viewing information about 87
system information
configuring 45
configuring with Configuration Wizard 35
System Status panel, using 16
system utilities
configuring 48

T

tables, sorting 16
task schedule
See schedule
temperature
configure controller shutdown for high 48
thresholds and policies, snap-pool 96
time and date
about 30
configuring 42

U

ULP 22
unique data (snapshot) 94
units for size representations 30
users
about user accounts 17
adding 40
change default passwords with Configuration Wizard 33
maximum that can sign in 16
modifying 41
removing 41
utility priority
configuring 49

V

vdisk
abort verification 82
aborting scrub 83
changing name 51
changing owner 51
configure drive spin down 51
configuring 50
creating 57
creating with the Provisioning Wizard 55
expanding 81
health values 89, 90
properties 87, 90
reconstruction 31
removing from quarantine 83
scrubbing 82
starting a stopped 117
status values 89, 91
stopping 116
verifying redundant 82
viewing information about 90

vdisks
about 18
configuring background scrub 48
deleting 58
viewing information about all 89
VDS and VSS providers
about 28
volume
aborting copy 68
aborting replication 115
changing default mapping 62
changing explicit mappings 63
changing name 52
configuring 52
configuring cache settings 52
creating 59
creating a copy 67
expanding 64
preparing replication by using the Replication Setup Wizard 110
properties 87, 92, 93, 97
removing replication from 114
replicating 112
replication addresses 120, 121
replication image properties 121
replication images 121
replication properties 120, 121
resuming replication 115
rolling back data 68
schedule properties 93
suspending replication 115
viewing information about 92
volume cache options
about 22
volume copy
about 26
volume mapping
about 21
changing default mapping for multiple volumes 60
changing explicit mapping for multiple volumes 61
properties 93
unmapping multiple volumes 64
volume masking 21
volume set
creating 59
volumes
about 20
deleting 60

W

WBI
about 15
communication status icon 16
session hang 16
signing in 15
signing out 16
web-browser interface
See WBI
write-back caching 22
write-through caching 22